INTERNATIONAL
HELLENIC
UNIVERSITY

Aligning the Operations of a Workout Club with GDPR

Karditsioti Nikoleta

UNIVERSITY CENTER OF INTERNATIONAL PROGRAMMES OF STUDIES

SCHOOL OF SCIENCE AND TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in e-Business and Digital Marketing

January 2021

Thessaloniki – Greece

Student Name:	Karditsioti Nikota
SID:	3305180013
Supervisor:	Prof. Dimitrios Karapiperis

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

January 2021

Thessaloniki - Greece

Abstract

Nowadays the percentage of data generated is much higher compared to the previous decades. The vast amount of data which are processed and handled by enterprises in daily basis, have create the need of personal data protection. The data comes from various sources (CCTV, registration forms etc.) but the largest volume of data comes from the Internet user's activities. When a company processes personal data of EU citizens, it is obliged to comply with the GDPR. The Regulation have introduced new obligations for enterprises that is necessary to be implemented. In case of non-compliance with the regulation the companies may be forced with penalties and fines. The purpose of this article is to analyze and present the need of the Regulation, as well as the changes that is required to be implemented both in company's activities in its physical daily tasks and on the Internet interface. Specifically, is going to be examined the personal data which is processed by a workout club in Thessaloniki according to data collection, process and storage. Last but not least, after the recording of the current situation and based on General Data Protection Regulation will be reported the necessary measures that have to be completed in order the Gym will be compliance with the GDPR.

This dissertation was written as part of the MSc in e-Business and Digital Marketing at the International Hellenic University.

Karditsioti Nikoleta

2021

Acknowledgements

In this section, I would like to thank my Supervisor, Prof. Dimitrios Karapiperis, for his valuable support and encouragement over the duration of my research study. I was motivated to complete my dissertation by his willingness to guide and support me, his availability whenever I was facing a problem and his targeted guidance during this challenging time of my study. His cooperation and guidance were valuable to me.

Contents

List of Figures

Introduction

It is indisputable that over the last 30 years, the technology has change dramatically people's daily lives and activities. The new era creates the need of specific rules that will protect the personal data and rights of citizens. In 2016, agreed upon by the European Parliament and Council that General Data Protection (GDPR), will replaced the Data Protection Directive which is a set of principles that were applied since 1995 until 2018. Since May 2018, all who process and handle personal data requires to comply with GDPR. GDPR requires information processors, across all industries, to be transparent and informative about their privacy practices. In this paper is going to be examined and analyzed the operations, the data collection and the processes of a workplace & wellness club in Thessaloniki. Last but not least, based on General Data Protection Regulation will be reported the necessary steps that the Gym has to complete in order to be complied with the Regulation.

Chapter 1: Big data mining infrastructure, application, platform, and data privacy issues

1.1 Understanding Big Data

Big Data is a large amount of data and information that is difficult and almost impossible to process with traditional methods of analysis. Big data refers to complex and large data sets, both structured and unstructured that can be analyzed to bring value. The needs of era and the shift of more and more businesses into e-commerce further enhance data production. Nowadays, companies receive millions of customer transactions. It is obvious that, the volume of the data which is required to handle every day is vast [1],[2],[3].

According to Gartner,

"Big data" is high-volume, velocity, and variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."

There are lot of definitions according to big data. What characterize big data is 5Vs which are volume, velocity, variety, veracity, and value [4] (Fig.1).

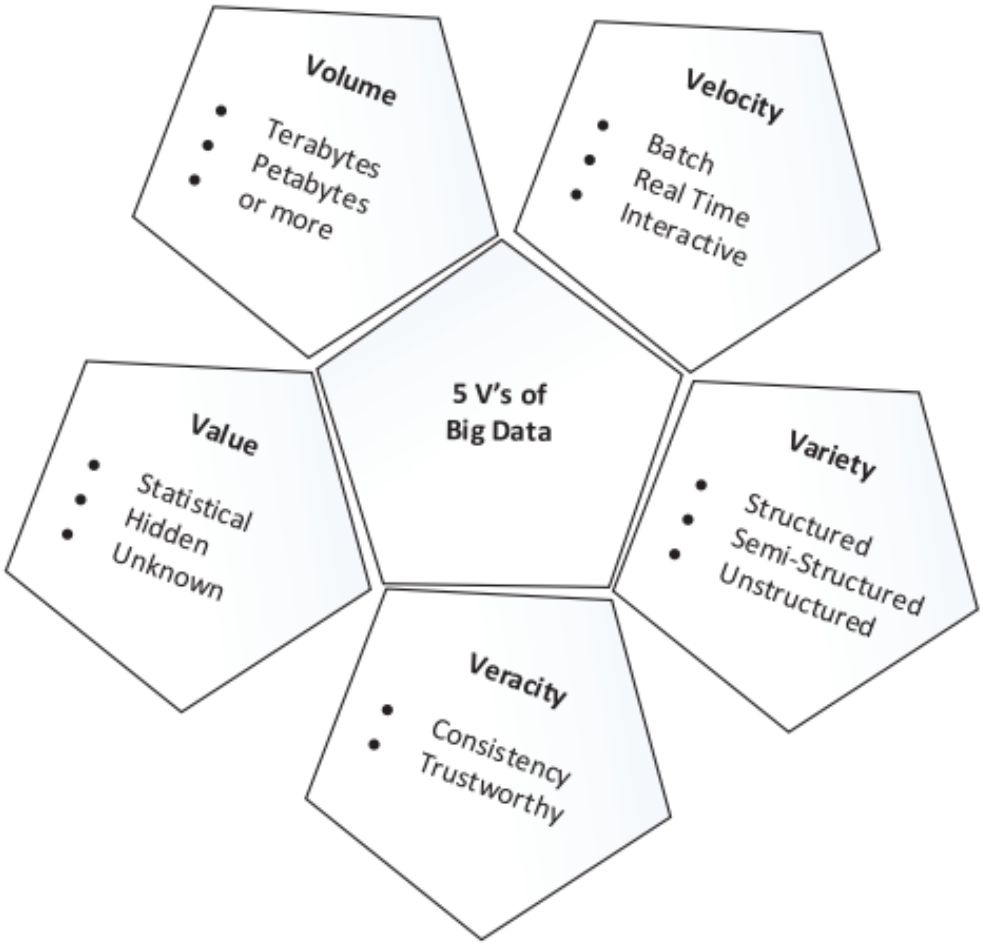

Figure 1_5Vs of Big data

- **Volume**: Vast amounts of data, used to be measured the scale of gigabytes (GB), although nowadays is measured zettabytes (ZB) and more (YB).

Today, Facebook alone ingests 500 terabytes of new data per day. According to IBM every day 2.5 quintillion of bytes of data are generated: this sums up to 4 zettabytes of data worldwide in 2013 [1],[4], and further enlargement is expected with the 50 billion of sensors going online by 2020.

- **Velocity**: Is the speed in which the data is accessible. Real time streams of data flowing from diverse resources (e.g., physical sensors or "virtual sensors" from social media, such as Twitter streams) [1],[4].

For instance, online data can be harvested and captured at thousands of events per second. Analytics algorithms can provide market trends and predict user behavior in microseconds. Sensors continuously generate massive production of logs [4].

- **Variety**: Data from a vast range of systems and sensors, in different formats and datatypes.

Figure 2 _ Big Data Variety

Numerical data, categorical data, geospatial data, 3D data, audio and video, unstructured text, including log files and social media, all form part of the big data ecosystem [4].

- **Veracity**: Describes the incompleteness (inconsistency, inaccuracy) of data.
- **Value**: Describes one of the biggest challenges of big data. It can be unstructured and includes so many different types of data.

There are some hidden patterns which can be identifying by big data characteristics. Big data is grouped into ten categories in terms of data type, data format, data source, data consumer, data usage, data analysis, data store, data frequency, data processing propose, and data processing method [4],[3],[1] (Fig. 3).

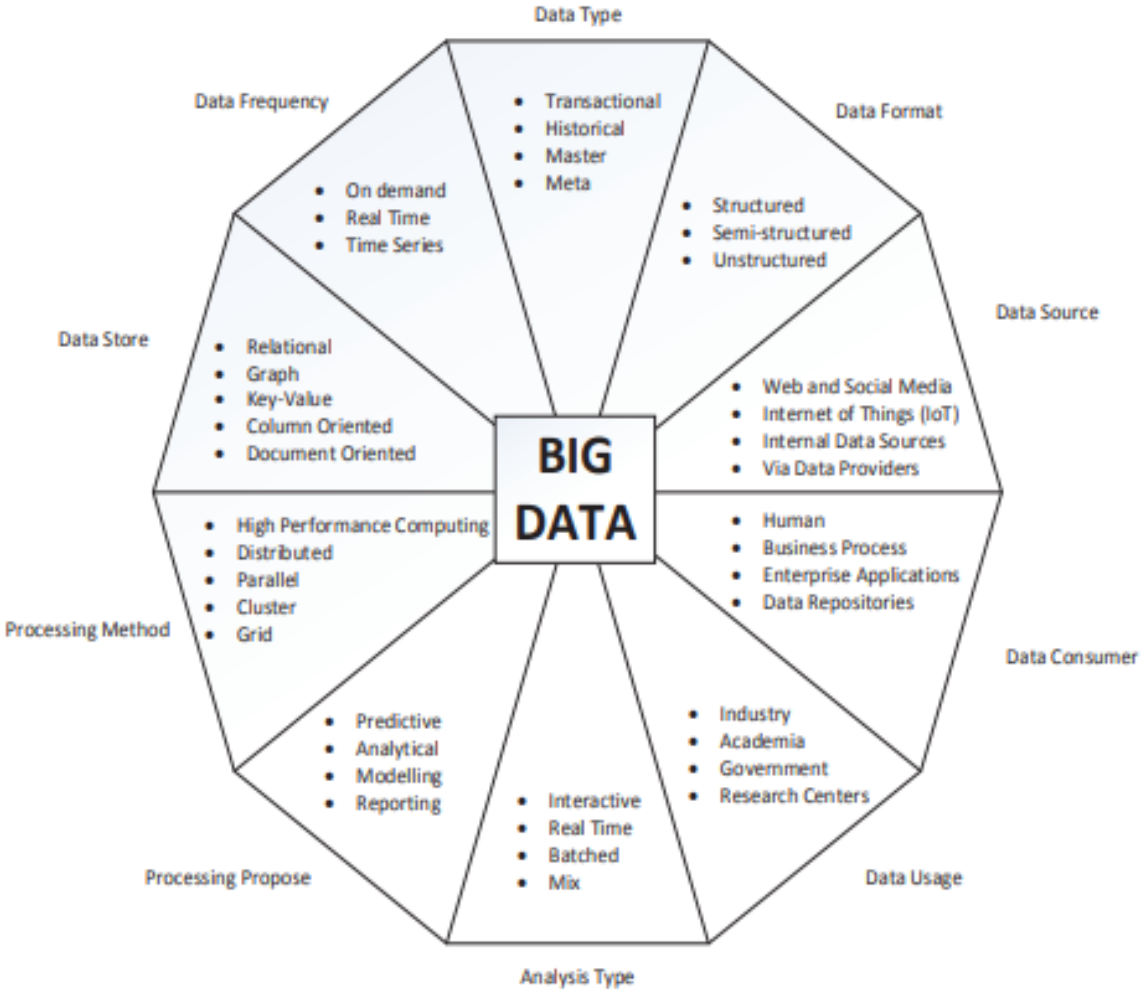

Figure 3 _ Big Data Classification

Having in mind big data characteristics, that are analyzed above, big data has become capital, with companies utilized them in order to improve their operations, productivity, and customer relations. Nowadays, huge amount of data is generated more and more. An important factor for this development is the cost reduction of sensors and mobile devises [1]. Moreover, people tend to use Internet, in dramatically higher rate compared to past. As a fact, people create everyday huge amount of data of various types and formats that is collected through many different sources such as online social media, Internet of Things (IoT), mobile devices, and genome projects via both wired and wireless communication channels. Nowadays, there are a numerous application of big data in almost every sector, including mobile communication, healthcare, police system, marketing, and retail, etc. [5].

Big data has created new opportunities and helped business productivity. However, big data has increased access to sensitive data that when processed can directly jeopardize the privacy of individuals and disrupt data protection laws. The usefulness of data processing is unquestioned for every enterprise, although it comes with high risks when operating personal and sensitive personal data [2]. First of all, the larger is the amount of data that is process the higher is the probability of re-identifying individuals even in datasets which seem not to have personal linking information. Moreover, big data analysis is capable to infer from "harmless" personal data new information that is more critical and was not intended to be revealed by the affected person.

1.2 Non-identifiable Data: The Common Mistake

In most cases, the results of big data analysis are statistical findings that are not connected to specific individuals. However, the definition of anonymity is a controversial issue. Even if the identity of the person to whom the data refers is not obvious, it must - before they be identified as anonymous - be thoroughly examined to see if the possibility of discovering their identity has indeed been "annihilated". A person may be directly identified from their personal information such as name, address, postcode, contact information, photograph, or some other unique personal characteristics or may be indirectly identifiable when certain information is linked together with other sources of information, including job title or workplace, salary, postcode or even the fact that they have a particular diagnosis or condition. Although identifiable parameters are not directly removed from a dataset, there is possibility to re-identify single individuals by the combination of the dataset with other information. This approach for de-anonymization is called ***background knowledge attack*** [7][8],[6],[9].

Below we will examine some of the most famous examples of re-identification.

Linking Attack

Sweeney,2012: Comparison of the voter list with the (anonymous) list of public hospital patients.

Figure 4_Linking Attack

For a specific date of birth, six people had the same date of birth. Three of them were men and only one with the same zip code. He was the (then) governor of Massachusetts.

According to this survey, 87% of the US population can be identified from the triplet "Tach. Code - date of birth - gender "[9],[10].

Netflix case study

In 2006 Netflix, the famous movie, and series platform, held a competition in order to improve their movie recommendation methods. As part of the challenge, Netflix released a dataset containing movie rating of 500.000 users. In the data sets he published there was no personal data, there was only subscriber IDs (without any connection to the actual identity) and movie ratings (score, movie info, date). Nevertheless, researchers with the help of other publicly available datasets, succeed to combine the information and were able to combine individual customers with high probability. The lawsuit end with more than $2,500 in damages for every of more than 2 million Netflix customers. Netflix pay $9 Million to settle the lawsuit [9],[10].

Genealogy Databases Enable Naming of Anonymous DNA Donors

In 2012, Yaniv Erlich with the help of his student Melissa Gymrek developed an algorithm to extract genetic markers from DNA sequences. Erlich and Melissa applied

the algorithm to an anonymized genome from a research database and doing some online sleuthing with some of the most famous genealogy sites. Eventually they found out that they could expose the identify of 50 donors [11].

Target Corporation_ Pregnant Algorithm

Target corporation is an American retail enterprise which is the 8th larger corporation in United States. One of Target corporation employees, Andrew Pole, developed an algorithm that was able to predict whether a woman was pregnant, observing online behavior of the user, online orders, clicks etc. In 2002, this algorithm by using behavioral advertising techniques, manage to identify a pregnant teen girl from her web searchers, ever before her parents understand it, and sent her a relevant voucher at her home [12].

1.3 Big Data Analytics

The term "big data analytics" refers to the whole data management lifecycle of collecting, organizing, and analyzing data to discover patterns, to infer situations or states, to predict and to understand behaviors.

Its value chain includes several phases that can be summarized as follows:

- **Data Acquisition/Collection:** The process of gathering, filtering, and cleaning data before storage and data analysis. Examples of potential sources are mobile apps, social networks, online retail services, wearable devices, public registers etc. The main purpose of data acquisition is to maximize the amount of available data and the process is based on fast and massive data collection.

- **Data Analysis:** The process of systematically applying statistical and/or logical techniques to collected data in order to utilized them for decision making as well as domain specific usage. The most challenging about big data analysis is the recognition of valuable data. Data analysis covers structured or unstructured data, with/without semantic information and may have multiple levels of processing

and different techniques (e.g., diagnostic, descriptive, predictive and prescriptive analysis).

- **Data Curation:** The active management of data over its lifecycle to make sure it meets the required quality requirements for effective usage.

- **Data Storage:** Storing and processing data in a way that can gratifying the needs of applications and analytics, that are required to access data. There are various ways to storage data, although nowadays the most popular and useful way is cloud storage. Cloud storage is that the trend but, in many cases, distributed storage solutions would be best options (e.g., for streaming data)

- **Data Usage:** Refers to the use of the data by interested parties and is very much dependent on the data processing management. For instance, the results from an analysis on trends in mobile apps usage could be available for the general public or restricted to a mobile service provider who commissioned the study. Therefore, big data users are possible to vary from a single organization to a wide range of parties, such as banks, retailers, advertising networks, public authorities, etc. Many activities of everyday life contain analytics, which fuel in return during a number of our everyday transactions. Some usual examples include [13]:
  - In hospitals, the comparison of patients' vital signs with historical data can identify patterns and extract useful information for early detection and treatment of diseases.
  - Mobile fitness apps collect data (sleeping patterns, time of walking and other streams of data), which if combined with other kind of data (e.g., health data) will become helpful tool for healthcare providers in order to offer better wellness programs.
  - Companies offer smart home functionality that enables motion detection to monitor what is happening in one's home and remotely control devices via a smartphone app.

- During our everyday travelling through the city, location information is sent by our smartphone regarding where we are and how fast we move, in order to get information about nearby points of interest.
- Google's self-driving car is analyzing huge amounts of data from sensors and cameras in real time to stay safely on the road.
- Smart TVs can track what we watch and provide accordingly suggestions or ads based on our preferences.

As it is obvious from the above, different stakeholders are involved in the variety of phases in the big data value chain, including hardware, software and operating system vendors, different types of service providers (telecom operators, social networks, cloud providers, etc.), analytics providers, data brokers, public authorities, etc. These stakeholders may take roles during a big data analytics scenario and interact with each other in different ways [14],[15].

1.4 Privacy and Big Data: what is different today?

As mentioned above, people tend to create more and more data, which is either in the cloud environment of applications (social media platforms, online banking, google applications etc.) or in a physical or electronic file of companies. Data privacy issues are capable to cause a dramatic reputation or economic damage to individuals and more especially to businesses.

Increasing use (and abuse) of personal data puts data privacy at the top of business's risk management agenda. It is a challenge that every business should accept in order to survive into the future IoT world.

Analyzing data so as to support deciding, discover trends or open new business opportunities is not new. The EU legal framework on data protection is aimed exactly at handling this collision by regulating the boundaries within which personal data are often processed with reference to the individuals' private life and knowledge. So, what is new about big data? The size is in terms of volume, variety, velocity and veracity, all the Vs of the large data definition, and their combination in analytics technologies. to

the present end, the most privacy challenges related to big data, overrunning the privacy concerns of "traditional" processing, are as follows [16]:

Lack of control and transparency

The collection of big data is based on so many different and unexpected sources that control by the individual can easily be lost, as in many cases he/she is not even conscious of the processing or cannot trace how data are flowing from one system to a different one. This poses significant engineering challenges on the way to effectively and timely inform users and on who is responsible of this task, especially when the processing requires the interaction of the many players.

Examples of such unknown and uncontrolled processing include data captured from sensors and cameras, from screening posts in social networks or from analysis of web searches.

Data reusability

One among the most targets of massive data analytics is to use data, alone or together with other data sets, beyond their original point and scope of collection. The scalability of storage allows for potential infinite space, which suggests that data are often collected continuously until a replacement value are often created from insights derived out of them. for instance, mobile apps providers collect personal data so as to supply users with information about their fitness or health status (e.g., heart disease, dietary habits, etc.). These data are often valuable to insurance companies and/or other providers (e.g., fitness centers, health consultants, etc.) who may target specific users.

Data inference and re-identification

Another important element for big data is that the possibility of combination data sets from many various sources, so be extracted more (and new) information. This also triggers privacy risks.

For example, it is feasible by combining various allegedly non-personal data to infer information related to a person or a group [17]. If the possibility of such inference is

high, there is be the case that an unintended processing of personal data occurs. In the same way, the combination of anonymized data sets and advanced analytics can lead to reidentification of a person by extracting and combining different pieces of information [18],[6].

Data inference and re-identification may in certain cases seriously affect an individual's private life. For instance, leading to humiliation or even threat to life due to the disclosure of confidential information. Data inference and re-identification may in certain cases seriously affect an individual's private life, for instance resulting in humiliation or maybe threat to life thanks to the disclosure of confidential information.

Profiling and automated decision making

The analytics applied to combined data sets aim at building specific profiles for people which will be utilized in the context of automated decision-making systems, e.g., for offering or excluding from specific services and products. Such a profiling can in certain cases cause to isolation and/or discrimination, including price differentiation, without providing the individuals the likelihood to contest these decisions. Furthermore, profiling, in the case of supported incomplete data, can cause false negatives, unfairly depriving individuals from rights and benefits that they are entitled to. One evident example of profiling today is the whole area of online behavioral advertising, which is also closely related to price differentiation (perceived by the willingness of people to pay) [19].

An additional example is that of profiling in predictive police algorithms, which may cause to discrimination of people, alike based on the place where they live.

On top of the risks mentioned above, one additional challenge in big data is the difficulty in enforcing, and/or monitoring the data protection controls. These difficulties are almost like those of cloud computing, for instance in reference to the situation of the data and therefore the possibility to conduct audits. Still, in big data there is one additional and important element: the involvement and interaction of different diverse stakeholders, which makes it even tougher (for regulators, data controllers, and users) to identify privacy flaws and impose relevant measures.

Chapter 2: GDPR: Innovations and New Obligations

2.1 GDPR - Definitions and Terminology

The EU General Data Protection Regulation (GDPR) is a landmark in the evolution of the European privacy framework. GDPR is series of rules designed to protect EU citizens personal data. It is relevant to all organizations inside the European Union (EU), the European Economic Area (EEA) and to organizations from other countries, if they process data of European citizens. Thus, the GDPR has effect on the biggest enterprises worldwide. It aims to simplify the regulatory environment for business so both citizens and businesses within the European Union can cash in of the digital economy. The new era of big data mining maximizes the need of data protection. Driven by this need, based on the concept of a privacy as a fundamental human right, GDPR has become a controversial issue about all the companies and citizens that use or manage data [20].

Personal data are information that, directly or indirectly, can identify an individual, and specifically includes online identifiers such as IP addresses, cookies and digital fingerprinting, and location data that could identify individuals. Centrally, the majority of everyday life aspects revolves around data. From social media companies, to banks, retailers, and governments - almost every service we use involves the gathering and analysis of our personal data. Personal information such as name, address, credit card number and more all collected, analyzed and, perhaps most importantly, stored by organizations. Sometimes, personal data refers to a set of “special categories”, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic etc., that must be treated with extra security. This kind of special data is called, sensitive personal data. Sensitive personal data should be held separately from other personal data [21],[20].

Individuals as consumers, citizens, customers, employees, patients etc., must have the means to exercise their right to privacy, as well as to protect and safeguard their

personal data from any misuse. The protection of personal data contains the preservation and protection of the fundamental right to privacy of every individual, which is abused by GDPR. With GDPR compliance, organizations have to ensure that personal data is gathered legally and under specific and rigorous conditions, and those who collect and manage it, are obliged to protect it from misuse and exploitation [20].

The GDPR has six general data protection principles [22],

- fairness and lawfulness
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality

but data protection by design and default is at the core of the GDPR. It is supported on one side by transparency (through ensuring full information is provided to individuals in an accessible style and manner) and on the opposite side by accountability (ensuring that all organizations take demonstrable responsibility using personal data) [20],[21].

The purpose of the Regulation is to protect all EU residents from any gaps and omissions in relation to the use of their personal data. The GDPR is a huge change in the operations of public and private sector actors, as it gives extensive authority to the competent authorities to control the way our personal data is managed and processed, regardless of the country in which the person in charge is located [20].

2.2 GDPR Key Terms

There are some basic key terms according GDPR that are presented below [20],[23],

This is the broad term for any information related to an individual or 'Data Subject', that can be used to identify the person directly or indirectly.

Figure 5_Personal Data

Sensitive Personal Data.

Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as "special categories" of personal data. The special categories are [20],[23]:

- Personal data revealing racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Data concerning a natural person's sex life or sexual orientation.
- Processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the GDPR.

Encrypted Data

Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access [25],[20].

Processing

An automated or non-automated action performed on personal data, for example collecting, storing, customizing, modifying, retrieving, retrieving information, using, deleting, organizing, registering, etc. In order for legal processing of personal data under the GDPR companies need to identify a legal basis for this action.

Profiling

Profiling is any kind of automated processing of personal data that involves analyzing or predicting your behavior, habits, or interests.

Data Controller

A "data controller" refers to an individual, company, or other body which decides the purposes and methods of processing personal data [23],[20].

Data Processor

A "data processor" refers to a person, company, or other body which processes personal data on behalf of a data controller.

Data Protection Officer (DPO)

An enterprise security leadership role required by the overall Data Protection Data Regulation liable for overseeing data protection) strategy and implementation to make sure compliance with GDPR requirements [23].

Data Erasure

Also known as the **Right to be Forgotten**, entitles the data subject to have the data controller erase data subject's personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Record of Processing Activities

It is written documentation of procedures concerning personal data of the processing activities that take place in a company. It demands that the records need to be in writing, including in the electronic form.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

2.3 Exploring the GDPR – why has GDPR been implemented?

The full text of GDPR is comprised of 99 articles, setting out the rights of individuals and obligations placed on businesses that are subject to the regulation. GDPR's provisions also require that any personal data exported outside the EU is protected. In other words, if any European citizen's data is touched, you better be compliant with the GDPR. For example, a U.S. airline is selling services to someone call at the United Kingdom, although the airline is found within the U.S., they're still required to suits GDPR due to the European data being involved. According to the EU's GDPR website, the legislation is designed to "harmonize" data privacy laws across Europe, providing greater protection and rights to individuals [20],[21].

Before the web, Europe has long been the model for a way our data should be protected and controlled. The reason is that the public's concern over privacy has dominated the business sphere, ensuring that stringent rules on how companies use the personal data of its citizens is always considered.

There have been rules about Data Protection since 1995. In April 2016, the European Parliament adopted the GDPR, replacing its outdated Data Protection Directive. Like many regulations and statutes throughout the EU and U.S., these regulations have not been able to keep up with the pace of the levels of technological advancement. With the GDPR regulation, all of 28 EU countries were forced to comply with the regulation, something that is not in line with the previous directive.

The issue with the Directive is that it is no longer relevant to today's digital age. Its provisions fail to address how data is stored, collected, and transferred today—a digital age and big data [20],[21].

2.3.1 Personal Data Breaches

Unfortunately, thanks to the actions of a number of most trusted companies, GDPR has become an important step in ensuring the protection citizen's and employee's data. Below, are presented some of GDPR breaches [29],[30].

Data Breach of Wonga Loans

Affected: 250,000 customers

The payday loan firm Wonga has suffered a data breach which may have affected up to 250,000 customers in the UK. The stolen information includes names, addresses, phone numbers, bank account numbers and sort codes.

Data Breach of Morrison's Supermarket

Affected: 100,000 employees

Supermarket chain Morrison's fell victim to an indoor attack that led to 100,000 employee's personal details being leaked. The cause was Andrew Skelton, one of Morrison's employees, who leaked the payroll data of Morrison's entire workforce, including bank account details and salaries. Thousands of staff have been awarded compensation payouts. The attack is reported to have cost the supermarket chain two million pounds and Skelton is serving eight years for the crime.

Data Breach of LinkedIn

Affected: 165 million accounts.

Social media platform, LinkedIn, suffered a data breach that compromised the private information of 165 million user accounts. The data has since been reported as up purchasable on the dark web marketplace. The data breach, which cost the corporate over three million pounds to wash up, has widely been reported because the results of weak user passwords and a failure on LinkedIn's part to protect the data [29].

Data Breach of H&M's Service Center

In October 2019, following an error in the company's Information System, users of the system gained access to a huge database, which contained extensive information about the privacy of employees of the service center in Nuremberg. After appropriate research were found out that, since at least 2014, parts of the workforce have been subject to extensive recording of details about their private

Moments and lives. Related notes were permanently stored on the network drive. Moreover, were took place "Welcome Back talks", as they used to call them, in which the employees after any kind of absences (vacation, sick etc.), were enforced to discuss with the supervisor team private sensitive issues which were also stored and sometimes were discussed on the floors of enterprise.

The H&M was fined with 3.5 million euros and was commitment for employee compensation [28].

Data Breach of Zoom

In April of 2020, the credentials of over 500,000 Zoom accounts were found for sale on the dark web and hacker forums for as little as $.02. Personal Data of zooms users, such as email addresses, password, personal meeting URLs, and host keys were collected through a credential stuffing attack.

Data Breach of Facebook

In the April of 2020, almost 267 million Facebook profiles have been listed for sale on the Dark web, all for $600.

From the above it is clear that the GDPR implementation was extremely necessary.

2.4 GDPR and New Obligations.

The Regulation introduces significant changes to the previous legal regime for the protection of individuals regarding the processing of their personal data and establishes increased obligations for any organization that processes personal data.

The process of the data has to be characterized of transparency. The purpose of the data has to be specific, legal and to be limited to the data necessary to fulfil this purpose. It must also be based on one of the following legal grounds [28],[30].

2.4.1 D.P.O - Data Protection Officer

The Data Protection Officer is mandatory according to GDPR. The D.P.O is independent and monitors the company's compliance with the Regulation as well as at the same time being the point of contact with the supervisory authority. His role is advisory (not decisive), and he does not bear personal responsibility for non-compliance with the Regulation [23],[31].

The Data Protection Officer informs the controller of his / her obligations, monitors compliance with the regulation, provides advice on impact assessment, cooperates with the supervisory authority and acts as a point of contact with it for processing issues.

2.4.1.1 Which organizations should designate DPO

The set of DPO is mandatory when [23],[31]:

- Processing is carried out by a public authority or public body (including natural or legal persons under public or private law exercising public authority). Courts are excluded when acting under their jurisdiction.
- Regular and systematic monitoring of data subjects on a large scale (e.g., insurance or banking services, telephone or internet services, provision of security services, all forms of monitoring and "profiling" on the Internet, such as for behavioral advertising purposes).
- Large-scale processing of specific categories of data (e.g., in the context of the provision of health services by hospitals) or personal data relating to criminal convictions and offenses.

Even when the designate of a Data Protection Officer is not mandatory, his / her voluntary set is recommended.

The Regulation does not provide specific criteria or certifications for the selection of the Data Protection Officer but considers that he has to be a person with extensive experience in personal data legislation and the management of any relevant infringements [24].

Therefore, the Data Protection Officer is appointed based on professional qualifications and in particular based on his or her expertise in the field of Law and computer data protection practices. He may be a staff member or perform his duties under a project contract with particular regard to dealing with conflicts of interest [23],[30].

2.4.1.2 What are the duties of a DPO?

The DPO promotes a culture of personal data protection within the organization or firm. The minimum tasks of the DPO are the following [23]:

- Inform and advise the organization and its employees on their obligations under the Regulation and other data protection provisions.
- Monitor internal compliance with the Regulation and other data protection provisions (e.g., identification and management of processing activities, staff training, internal audits).
- Provide advice on impact assessment and monitor its implementation.
- Be the first point of contact for supervisors and data subjects (employees, customers, etc.).
- Cooperate with the supervisory authority [23].

2.4.2 Further Obligations of GDPR

Data Controller

The data controller determines the needs and therefore the means by which personal data is processed. So, if your company/organization decides 'why' and 'how' the personal data should be processed it is the data controller

The company/organization may be a joint controller when alongside one or more organizations it jointly determines 'why' and 'how' personal data should be processed. Joint controllers must enter an appointment beginning their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed [20],[23],[31].

Notification of Data Breach

Notification of data breach:

To the supervisory authority: In the event of a breach of personal data, the data controller, within 72 hours of becoming aware of the breach, disclose the breach of personal data to the supervisory authority.

To the individual of interest: When the breach of personal data may seriously endanger the rights and freedoms of individuals, the controller shall promptly notify the breach of personal data to the data subject [31].

For the notification of a violation case to the Authority, in compliance with the relevant obligation of no. 33 of Regulation (EU) 2016/679, the controller must complete a special form and submit it to the Authority [30].

Penalties and Fines

Violations of personal data can lead to fines up to 10,000,000 or in the case of companies up to 2% of the total global annual turnover of the previous financial year (whichever is higher). It is characteristic that even this absence of appropriate organizational measures for compliance with the Regulation can lead to this fine, without even a case of violation. Fines in special cases can become heavier and up to

€ 20,000,000 or up to 4% of the total global annual turnover of the previous financial year, whichever is higher [32].

Consent

The GDPR introduce new rules for processing data based to consent. The purpose of these rules is to ensure that the individual understands what he or she is consenting to. According to the Regulation the consent of the concerned individual should be

- Freely given
- Specific
- Informed
- Unambiguous by way of a request presented in clear and plain language.

In case of processing personal data pertaining to a child based on consent, then parental consent is required [20],[21],[32].

Right to be informed

Companies and Organizations must be completely transparent about the way and purpose of processing personal data. In order to ensure the fair and lawful processing of personal data, Data Controllers must provide at least some information to the individuals of interest regarding the collection and further processing of their personal data. This information must be concise, transparent, in a comprehensible and accessible form, using clear and simple language. Any information provided to children should be in clear and simple language that the child can easily understand [31].

Right to erasure ('right to be forgotten')

It refers to a person's right to request the deletion or removal of personal information. The data subject has the right to request from the controller the deletion of personal data concerning him. The data controller is obliged to delete personal data without undue delay, if one of the following reasons applies: a) the data is no longer necessary, b) revocation of consent, c) the subject opposes the processing, d) illegal processing, e) the data must be deleted on the basis of a legal obligation

Example: Recognizes the right of individuals to ask search engine service providers to delete search results that contain personal data concerning them [31].

Right of Access

The text subjects to do it indicate exactly what information was required to do, do and do something. The intangible assets of an organization (i.e., the application of the right should not require the disclosure of trade secrets, etc.). cases in which trade secrets and other intellectual property rights fall within the scope of access are rare [31].

Restrictions of Rights and Principles

Refers to the right of an individual to block or suppress the processing of his personal data. In some cases, people may not have the right to require the controller to delete their personal data but may restrict the purposes for which the controller may process this data (e.g., another person or entity, purposes that serve a significant public interest or for other purposes such as the person concerned may consent) [31].

Right of objection

The data subject is entitled to freely opposes data processing whenever it wants personal matters relating to it, including. The Data Controller after the objection is no longer edited personal data, unless it demonstrates imperative and legitimate processing reasons which outweigh the interests, the rights and freedoms of the data subject or the data is necessary for the establishment, exercise or legal support claims [31].

Revision Right of Automation

Profiling and automated decision making can be useful for data subjects, organizations, providing benefits such as increased efficiency and resource savings. However, these procedures require adequate safeguards, as they can pose significant risks to individuals' rights and freedoms. Individuals can choose not to be the subject of an automated decision if it has legal consequences [30],[31],[32]

2.4.1 Disaster Recovery and Contingency Plan

The Disaster Recovery and Contingency Plan is a document that describes in detail the organizational, technical and physical security measures taken to put the basic security principles into practice. It is essentially an implementation plan of what is theoretically described in the Security Policy and must cover the entire technological infrastructure and personal data processing systems of the company.

Due to its nature, it must be subject to regular reviews in order to fully respond to any modifications to the information systems and infrastructure. It should also include procedures for conducting annual audits, both internal and external, to check the effectiveness of security measures and to consider the need to review and supplement them [30],[31].

2.4.4 Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment (DPIA) is a process which is valuable for businesses in order to identify and minimize the data protection risks of a project.

When a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of processing, may pose a high risk to the rights and freedoms of individuals, the data controller shall, before processing, impact assessment of the planned processing operations on the protection of personal data. An assessment may consider a set of similar processing operations which involve similarly high risks.

2.5 Guidelines of GDPR

2.5.1 Consent of the subjects

The data subject should be always informed about the processing of his data and always obtain consent (where his consent is required) and save it [20],[32].

- **What does consent mean:** Consent is the written statement signed by the subject that he accepts the processing of his data for a specific reason, e.g., commercial, statistical, promotional, etc.

- **When consent is required?** Consent of personal data is required for any non-contractual processing purpose.

Special types of consent are formed depending on each case of marketing data processing, training, etc. In addition, it is mandatory to inform the subject about the processing of his data in each case of their collection.

Opt-in process

This process authorizes a customer or recipient of mail, email, or other instant message to a merchant to send merchandise, information, or more. After the positive agreement of the customer the merchant will continue to send material or messages until the recipient chooses to opt out. It is a process that requires the consent of the customer and is closer to the logic of consent as defined in the Rules [20],[31],[32].

Opt-out process

In this process, a customer or recipient of an e-mail, e-mail or other direct message to a merchant expresses the desire not to send information or more messages. It concerns the refusal of the customer to the merchant to continue sending material or messages. It is a procedure that does not fully cover the requirement of pure unaffected customer consent required by the Regulation [30],[32].

2.5.2 Instructions for the protection of personal data

- Identification of a subject before any information is given.
  The identification can be done using the 3 basic identification data that we have in our database such as ID number, TIN, Date of birth, Home address, etc.
- Do not transfer personal data outside of work in any way
- Always use legal lists to communicate with subjects
- If you receive any questions or complaints or grievances from any subject via e-mail, telephone, SMS, notify your DPO or manager immediately
- Printed documents and reports must be properly protected.

- Filing cabinets and cabinets must be locked\ Always use the document destroyer to destroy documents that contain personal data.
- Do not leave papers in a conspicuous place (clean office policy)
- We do not transmit; we send documents to anyone if we do not have a contract where a cooperation agreement has been signed and with confidential information
- We do not give telephone information to third parties
- We do not give information to an interested party unless he is certified to be himself or a person authorized by him
- Confirm the recipient's email address or address before sending any information.
- If you are sending e-mail to more than one recipient, use the separate BCC notification.
- We keep the physical files locked
- It is not allowed to photograph spaces, documents and offices

Chapter 3: Data Privacy Protection in Web Analytics and Digital Marketing

As have been mentioned above, the General Data Protection Regulation (GDPR) is a European law that governs all collection and processing of personal data from individuals inside the EU. Under the GDPR, it is the legal responsibility of website owners and operators to make sure that personal data is collected and processed lawfully. A website even if it is outside of the EU is required to be aligned with the Regulation in case of collection data from users inside the EU. Thus, it is great importance for every website owner to be well informed about all the registrations that is relevant with GDPR [31],[33],[34].

3.1 Website compliance with GDPR

According to GDPR, every kind of website (e-shop, portal, blog, even a small website of an enterprise) is obligate to comply with the GDPR rules, otherwise there are strict penalties.

Generally, the websites that have to comply with GDPR are those that collect, process and store data of their visitors / users. Below, is presented a list of website activities that are GDPR subject [34].

- Web Analytics
- Registration forms
- E-commerce functions that collect payment information, orders, etc.
- Newsletter subscription forms
- Scripts that use cookies
- Contact forms

3.1.1 10 Steps to Aligning a Website with the GDPR

Privacy Policy

A website's privacy policy should state in detail and clearly how users' data is collected, processed, and stored. In addition, it is important to indicate the retention time of the data and the way in which users can view and delete their data [31],[34],[35].

Encrypt data with SSL

The SSL (Secure Sockets Layer) certificate is the first step for the GDPR because it offers privacy and security in transactions and the transfer of user data. SSL is a form of security for sites that handle sensitive information such as visitor's personal information and credit card numbers. It creates a secure connection between a visitor's web browser and the server of the company they're interacting with.

Forms

If a website uses any type of forms (communication, support, sales, etc.) you will need to add consent boxes which should not be completed by default, but should be selected by the user, since the pre -filled boxes are not considered free consent. Users should be able to give different consent depending on the type of data processing that is done each time. For instance, if user data is provided to third

parties, another consent box should be added asking for the user's consent [35],[33].

Easy unsubscribe or revocation of license

Users should be able to unsubscribe or withdraw their consent from processes and actions that process their data. For example, users should be able to unsubscribe from the newsletter easily and at any time [35].

IP recording

If the IP addresses of users or visitors to a website are recorded, it should be mentioned in the privacy policy because IP addresses are "personal data" of individuals [35],[36].

Advertising on social media

Website members need to be informed and consent to the use of their emails in social media advertising campaigns.

Cookies

In case of using cookies, it is necessary that the visitors of the website will be informed when they enter it. They should also be able to disable cookies through the browser settings [35], [36],[38].

If have been used third party cookies, such as google analytics, should be mentioned to website's privacy policy.

Re-marketing

Re-marketing works with the use of cookies which "mark" and monitor the users of each site. Their use and mode of operation should be clearly stated in your site's privacy policy.

Online Payments

If payment gateways such as PayPal, Stripe, Sagepay are used for customers' financial transactions and their personal information is first passed through the e-shop of the website, they will need to encrypt this information via a SSL certificate.

Leakage of Information

The GDPR stipulates the duty of companies and organizations, in case of data breach, to notify within 72 hours the Personal Data Protection Authority of the country in which they are located [34].

3.2 Cookies

An internet cookie a.k.a. an HTTP cookie, is a small piece of data sent from a website that is stored on computer or mobile when a user is visited the website. Cookies themselves are usually harmless as they cannot infect computers with malware. They can even be helpful for both websites who use them and individuals visiting those websites. For example, when online shopping, cookies on ecommerce websites keep track of what users shopping for. If a user does not have that tracking, the cart would be empty every time that the user is moved away from that website.

For businesses/websites, cookies are often used for authentication (logins) and tracking website user experience. For example, tracking multiple visits to a website in order to provide to final users a better user experience. Although, there are some "bad" cookies as are called. These cookies contain personal data directly in the cookie itself. Use of cookies in these ways is considered bad practice nowadays because they are used to create profiles of the natural persons and identify them [37],[38].

3.2.1 Type of Cookies

Generally, there are different ways according cookies classification: their purpose, how long they endure and their provenance [37].

3.2.1.1 Provenance

First-party cookies. First-party cookies are put on user's device directly by the website.

Third-party cookies. These are the cookies that are placed on user's device, not by the website that are visited, but by a third party like an advertiser or an analytic system [37],[38],[43].

3.2.1.2 Purpose

Strictly necessary cookies

These cookies are important for a user to browse the website and use their functions, such as accessing secure areas of the site. For instance, strictly necessary cookies, are cookies that allows users to keep in cart their items during their online shopping. These cookies will generally be first-party session cookies. While it is not required to obtain consent for these cookies, what they do and why they are necessary should be explained to the user [37],[38].

Preferences cookies

Also referred to as "functionality cookies". These cookies allow a web site to remember the user's choices within the past, like what language, region, name, and password [37].

Statistics cookies

In addition are known as "performance cookies." These cookies select information about the duration of a user use a website, which pages are visited and which links are clicked on. None of this information can be used to identify user identity. It is all aggregated and, therefore, anonymized. Their main purpose is to improve website functions. This includes cookies from third-party analytics services as long as the cookies are for the exclusive use of the owner of the website visited [37],[38].

Marketing cookies.

These cookies track user's online activity in order to help advertisers deliver more relevant advertising or to limit how many times a user see an ad. These cookies may contact the information with other organizations or advertisers. These are persistent cookies and almost always of third-party provenance [38],[43].

3.2.1.3 Duration

Session cookies

These cookies are temporary and expire when the user close browser (or once session ends).

Persistent cookies

This category includes all cookies that remain on user's hard drive until are erased. The cookie can be deleted by the user or by the browser, depending on the cookie's expiration date. According to the e-Privacy Directive, they should not last longer than 12 months, but in practice, they could remain on the user's device much longer if the user does not take action [37],[38].

3.2.2 Cookie compliance

In order a website comply with the regulations governing cookies under the GDPR and the e-Privacy Directive have to:

- Receive users' consent before utilizing any cookies except strictly necessary cookies.
- Provide accurate and specific information about the data that is tracked by cookies as well as its purpose in plain language before consent is received.
- Document and store consent received from users.
- Make it as easy for users to withdraw their consent as it was for them to provide their consent within the first place [35],[31],[37].

Website owners have to decide the types of data they collect and whether that information is necessary in order to perform the task for which the information is being collected. According to article 5 of GDPR, collected or processed data must be limited to the minimum necessary amount in order to be achieved the purpose for which it is collected. GDPR also requires all personal data to be secured, so data encryption should be considered [35].

If have been used any kind of analytics program on website (e.g., Google Analytics), it is websites' owner responsibility to ensure it is compliant. Google has taken care of its side, although website owners have the responsibility to ensure that Web

Analytics will be combined with GDPR. If tracking data is collected that allows an individual to be identified – by their IP address for example – consent must obtain [31],[32],[38].

It is important that website visitors can get in touch with a site owner to utilize their GDPR rights and freedoms, so all contact information needs to be up to date. According to the Regulation, it must be easy for visitors to communicate with the Data Controller, they should have the ability to exercise their right to be forgotten, request a copy of any collected and processed data in order to check their personal data for accuracy. In case that a website visitor chooses to erasure their data, it is useful to have a mechanism in place that allows that automatically happen via the website.

It is necessary to properly informing the users about the cookies which are used in the website and receiving their consent.

As have been mentioned, website owners that fail to make a website GDPR compliant can face stiff financial penalties. The fine for noncompliance websites with GDPR is up to €20 million or 4% of global annual turnover (whichever is greater).

3.2.2.1 Fine of 30.000€ to an airline company for the cookies policy on its website

Fine of 30,000 euros was imposed by the Spanish Data Protection Authority on Vueling for the cookies policy used on its website.

According to the decision of the Spanish Authority, the company does not provide a cookie management system or configuration table that allows the user to choose which cookies will be used in a more detailed (granular) way.
To facilitate this option, the table should allow all cookies to be discarded via one mechanism or button, all activated via another or enabled to choose which cookies to install, allowing each user to manage his preferences.

According to above, the Spanish Data Protection Authority were proceeded to impose a fine of 30,000 euros on the company. [39]

3.3 Web Analytics

Web analytics are tools that measures and analyze the data in order to inform an understanding of user behavior across web pages. The main purpose of Web Analytics tools is to improve online marketing and business profits [44]. Analytics platforms measure activity and behavior on a website, for instance: how many users visit, how long they stay, how many pages they visit, which pages they visit, and whether they arrive directedly or not. Web Analytics is the collection, reporting, and analysis of website data through server logs or code embedded on webpages. The basic purpose of website analytics is to benchmark website performance and to track user behavioral data by creating and measuring Key Performance Indicators (KPIs). KPI is a type of performance measurement that helps the company overview and analyze its performance [40],[44].

Web analytics applications do only not measure web traffic but can become a valuable source of information that will be useful in business decision-making. Web analytics tools are also helpful in order companies can measure the results of traditional advertising campaigns. It can be used to estimate rate of traffic change after launching a new advertising campaign. Via Web Analytics tools, companies are able to gather information about the number of a website visitors or the number of page views. Furthermore, provides useful information about website traffic and popularity of trends, which are valuable in strategy marketing creation [44],[45].

3.3.1 Web Analytics used in EU

Google Analytics

For numerous clients, Google's analytics suite may be an extraordinary fit. It offers valuable data, including live website traffic data, insights about audience and integrations for other Google products like Adwords and AdSense. Despite the huge amount of information can be viewed, the layout is fairly straightforward [45],[46].

Open Web Analytics

Open Web Analytics (OWA) is an open-source web analytics software framework that can become a powerful tool for tracking and analyzing user's behavior in websites and applications. OWA is licensed under GPLv2 and adds easily to websites by using simple Javascript and PHP based APIs. Open Web Analytics offers a lot of the same features as other website analytics tools, with a few supplementary options. In addition to tracking live site traffic, referrals, and other expected metrics [45],[46].

Wix Analytics

Wix Analytics is an option for people looking for general website performance metrics as well as those looking for in-depth insights. It provides information on traffic trends. Wix Analytics provides an overview about where the visitors come from, the enter device, and online behavior of them. Also provides information about top customers, revenue analysis and traffic trends. These information are helpful for decision making and strategy optimizing [45],[46].

Adobe Analytics

Adobe Analytics provides real-time analytics for users across different marketing channels. Use a tag for all questions which are related to the user interface, implementation coding, and interpretation of reports including Adobe Dynamic Tag Manager (DTM), and Adobe Launch. It is a suitable option for processing multiple sources of data and not only websites data [45],[46].

Matomo

Matomo is an open-source analytics platform that offers just about anything you could want. Real-time data, event and content tracking, heatmaps, A/B tests, and more are all present. Matomo is quick to mention that users own 100% of their data, with "no external sources looking in." [45],[46].

3.3.2 Basic steps of the web analytics process

- **Collection of data:** In order to start the data analysis, it is essential to precede the data collection. In this stage take place the collection of the necessary data.
- **Processing of data into information:** After data collection it is important to transform the relevant data into information. **Especially**, this step involves transforming data into metrics by creating ratios. For example, bounce rate is dividing the early leavers count by total visitor.
- **Tracking KPIs:** As it has been mentioned above, KPIS are metrics which are important for business strategy. They supply history to key metrics so companies can measure how they are progressing over time.
- **Identifying online strategy:** In this step the main objective is the decision-making concerning the online goals, aims, and standards for the organization or business [43],[44].

3.3.3 Web Analytics Sources

The main aim of web analytics is to collect and analyze data related to web traffic and user's online behavior. The data mainly comes from four sources:

- **Website Visitors Data**
- **CRM**
- **Search Engines**

3.3.4 Web Analytics Reports

Web Analytics is a valuable source of information which is helpful in decision making process. Via Web Analytics marketers and companies' administrators have access to reports that create a total overview of business position. Below is presented characterized examples of Web Analytics reports [44],[45],[46]:

Audience Data

- Number of Visitors
- Number of Unique Visitors
- Returning Visitors
- Traffic over time
- Traffic by time of the Day
- Traffic by Device
- New vs Returning Visitors

Demographic Data

- Gender
- Location
- Age
- Language

Visitors Behavior

- Total Clicks
- Bounce Rate
- Page per Session
- Exit Page

Sales

- Top Sales (month, year etc.)
- Sales over Time
- Sales by item
- Sales by Location
- Top paying Customer

3.3.5 How does GDPR affects Web Analytics

3.3.5.1 The most important changes in Web Analytics

- **Consent for each data:** Accurate information must be provided to individual users. The type of data to be collected must be strictly stated, as well as the purpose of their collection. "Explicit" consent is a prerequisite [31].

- **Update processing policy**: a user consent form must be available to process his data, in an easy, accessible form and in clear and simple language. The privacy policy should reflect the following information in a clear and plain language:
  - ✓ What information is collected
  - ✓ Who is collecting this information
  - ✓ How is this information used
  - ✓ Who will this information be shared with
  - ✓ How you protect the information
  - ✓ How to correct any inaccuracy in this information
  - ✓ Contact information [31],[34]
- **IP Anonymization**
- **Right to "forget":** All subjects have the right to request the removal of their data from your business database [31].
- **Universal Compliance:** All vendors providing cloud services to businesses in the EU or processing data in any other way must meet the requirements of the Regulation.
- **Data Protection Officer (DPO):** If a company manages a large amount of personal data, it is required to designate a data protection officer [24].

3.6 GDPR and Social Media

A particularly interesting but also complex issue that should be considered according GDPR, is the protection of personal data in social networking services. Nowadays, majority of people have used, at least once, social networking platforms, posting some commentary or photos or sharing any personal information. Since anyone can voluntarily disclose any personal data that concerns them, defining the scope of responsibility of DPO and Data Processor. regarding the protection of the personal data of social network users, is a particular hard work [40].

3.6.1 Data protection in social media

Social networking services are online communication platforms, which allow their users to join user networks with similar ideas and which are constantly gaining ground, having a significant impact on our lives, resulting in more than one billion users. Examples of such services are Facebook, twitter, Instagram etc. The terms "social media" and "social network" are often synonymous with "social networking". However, there is a significant difference: the term "social media" refers to social media tools, while the term "social networking" refers to the process of social networking.

3.6.1.1 What are their common features?

- Users are required to give personal information to create a description of themselves or a "profile"
- Social networking services also provide tools that allow users to post their own content (user-generated content, such as a photo or calendar entry, music or video clips, or links to other websites)
- "Social networking" is accomplished by tools that provide a contact list for each user that users can get in touch.

3.6.1.2 Who is considered the data controller?

Social media providers are, in principle, responsible for processing user data. They determine the purpose of processing the data of its users, while providing the means for this processing, as well as all the "basic" functions related to user management (e.g., creating and deleting accounts). According to a recent ruling of the Court of Justice of the EU, the page manager in a social networking service can also be considered responsible for processing.

3.6.1.3 As data controllers should:

- Provide adequate warnings to users about their privacy risks when they download information through the social networking service

- Remind social media users that uploading information about other people may be in violation of their privacy and data protection rights
- Advise users not to upload photos or information about other people without the consent of them [24],[23].

3.6.2 Social Media and Advertising

Social media providers determine the use of user data for advertising and marketing purposes - including third-party advertising. In particular, they earn a large portion of their revenue through advertising, which is provided in parallel with the websites created and / or used by users. Users who post a lot of information about their interests in their profile are a niche market for advertisers who want to provide them with targeted ads based on that information. It is therefore important that social networking services operate in a way that ensures respect for the rights and freedoms of users, who have the right to expect that the personal data they disclose is processed in accordance with European and national legal protection privacy and personal data.

In addition, one important feature is the use of cookies. The use of cookies is particularly widespread on social media. So, it becomes clear that if a user expresses their preference for a product or service, such as by clicking the like button on Facebook or a similar one on other platforms, they will immediately start receiving notifications about similar products. The difference with GDPR is that the users now has an even stronger right to prohibit these practices at any time and the provider must immediately stop using their data. In any case, the users must always be informed of their right and prohibit the use of their personal data the first time the provider ask them the relevant question [35].

3.6.2.1 Case study Facebook: Personal Data, Tools and Application

Facebook is an online platform which is proceed user's personal data. In most cases it is quite obvious to the user which of the data he has provided is actually managed by Facebook and which is not. However, there are cases in which it is not clear enough what data the user provides to Facebook for processing.

Content and Metadata

Facebook collects information from the user's content that is uploaded, as well as from all his activity on the platform. Specifically, beyond the information that is related with a post (metadata- location, date of post, type of post, duration and frequency of such posts) the platform also collects regional information. For instance, Facebook collects data from the content of the post as well as from posts made by other users about the same user (e.g., posting on his wall, comments, sending a personal message, tag in a photo or other post). Moreover, the frequency in which a user chats with another person on Facebook is also an element that the platform collects, as well as the frequency that users visit a page or another user's profile.

In addition, Facebook collects information about the pages that each user follows or likes. Based on these interests, the platform suggests friends and other pages or even more groups that are directly related to user's specific activity (e.g., suggests friends from the members of the page or group, suggests other pages in which the members have subscribed, etc.). Furthermore, Facebook provides the ability synchronize the user's contacts with their Facebook account. In this way, it is also possible for Facebook to use the phone number to identify the profile of a user with whom another user has just spoken over the phone to suggest him / her as a friend on the social network. All these data can be used for advertisement purposes.

Facebook affiliate with other Websites

As mentioned above, apart from the information provided by users with their consent to the social networking platforms, there are many other ways in which, platforms such as Facebook, have access to information that concern users and to which they have agreed by accepting the terms of use and privacy of the social network. One of them is the like button or the share button (social plug-in) found on many websites or e-commerce websites. With these tools (or services as the platform calls them) and regardless of whether the user who visits the respective website clicks on the relevant icon, the website collects information about its browsing.

As stated in the terms of use, Facebook collects the unique user code (user ID), the information that the visit to the specific website took place, the time and date of the visit as well as information about the browsing, which are all collected through

cookies. If the registration to a website become through the Facebook account and the user makes use of this option, then Facebook also collects the relevant information that notifies the user with a relevant pop-up message. Facebook uses the relevant information in order to customize the user's profile and especially for advertisement purposes.

Ads and Applications

Facebook ads work in a fairly simple way, as described above, which makes them particularly attractive to different types of advertisers who want to promote their products or services. By using these tools, the advertiser can specialize or expand his audience according to his goals and the amount he wishes to allocate. The information about the user's interests Facebook identifies from the relevant field of interests, from the groups to which it belongs and from the pages that it follows. The same thing happens when a user performs a search on another site and then logs in to his Facebook account. If the website uses the relevant tools, Facebook will receive information about the user's preferences using cookie technology and will advertise relevant content to the user. For example, if the user is looking for accommodation through a relevant accommodation site and the site uses the relevant Facebook targeted ads tools, then the user's homepage will display an ad about the user's previous searches on the site.

Facebook Insights and Non-Identifiable data

Facebook enables Facebook page administrators to collect anonymous information about the characteristics and habits of people who have visited fan pages, enabling them to target in better way their communication with users and customers. With the help of cookies are able for administrators to extract statistics about the user's habits, preferences and needs. This data is used by marketers and individuals who advertise on Facebook to reach their audience with more targeted ads and related content. It is an important notice that, the page administrator may not know which specific user has performed a particular activity, but the information is used to target new ads.

With GDPR and the restrictions it imposes on the use of tools for the purpose of drawing up profiles and monitoring user behavior, the data that managers can collect

will change dramatically. Certainly, of course, the clear information and full consent of the user will be required to provide his data for such purposes.

Chapter 4: Case Study ¨the Gym¨

Methodology

Multiple methods were used to capture existing information systems and physical security measures such as:

- On-site Mapping: Multiple visits were taking place to the Gym in order to record the operation of the services and structures, regarding the processing of personal data from the available information and technological means.
- In-person Interview: In-person interviews were conducted with both administrative and technical staff.
- Targeted Questionnaires: Specialized and targeted questionnaires were completed by the technical and administrative staff as well as from data controller of the Gym.

4.1 Description of ¨the Gym¨

In the framework of the dissertation, we will study a medium enterprise of a gym in Thessaloniki. For the sake of brevity from now on we will call it ¨the Gym¨. The Gym is located on the east side of Thessaloniki. It is one of the most popular gyms in town with a large number of members.

According to the Article 5 of GDPR the collected data must not be easily accessible and visible. The Gym has six computers that are used by the employees and they are connected to a central server and on the Internet. All of them have password that is known only by the Gym employees.

In addition, the Gym is the administrator of two websites. The first has to do with the presentation of the Gym and its facilities. There is a description of its services and staff and the presentation of photographic material. The second is a website that provides real-time training and on-demand training services. In this case, the Gym collects data during registration, as well as throughout the time that users use the service as it records the lessons.

According to Article 30 requires written documentation of procedures concerning personal data which is processed within a company. It demands that the records need to be in writing, including in the electronic form. Based on the Gym record of processing activities, below are analyzed the relevant activities and data that concerns the Gym members.

4.2 Registration of users who have access to information systems

Users of the service systems can be grouped into internal users, especially permanent or temporary employees who respond to the internal activities and processes of the service, technical support staff and external service partners who can access the applications and services.

- Permanent or part-time employees belong to the following areas:
  - ✓ In the Gym administration department
  - ✓ Gym Instructors
  - ✓ Cleaning staff
- The technical support staff is responsible for the efficient and secure operation of the company's information systems.
- The external partners of the service who have access to the information systems of the service.

The gym has 30 permanent employees (19 instructors, 5 administrators and, 6 cleaners) of whom 80% (24 employees) have access to personal data and sensitive personal data. The Gym collects data from its members in various ways. For member's safety, it is necessary to collect and process both personal data and sensitive personal data. The Gym processes and stores the data in physical files and electronic with the help of a CRM platform. The CRM platform is provided to the Gym by an external partner, which is the data processor. Moreover, the security service is provided by an external company. Last but not least, the Gym corporates with two external partners about the technical support.

4.3 Data Collection

As it is mentioned above, the enterprise collects various data with different means. According to the Article 5 of the General Data Protection Regulation, it is necessary the data subjects to be well informed about the collected data, the reason of the collection, the process of it as well as and the time period that will be stored.

4.3.1 Closed-circuit television (CCTV)

Inside the building there is Closed-circuit television (CCTV) of 15 cameras, which are recording 24 hours a day, and the data is stored by a security company, which is an external partner of the Gym, and the data is stored for one month. The cameras do not record voice. There is not notification about cameras, and members are not informed about the recording. Although there is any notification about the third partner and the period that the collected data is stored.

4.3.2 Registration of physical members

The Gym collects data of members during the registration process. According to article 6 of GDPR the data subject has to be consented to the processing of his personal data for one or more specific purposes. Initially, Gym members it is necessary to fill in two documents. The first is the Registration Contract, in which they have to state personal information (name, telephone number, e-mail, date of birth), demographic data, and VAT number. Last but not least, the members are asked for their consent about the use of their photo on their profile and if they accept to receive advertising messages and newsletters. Then, before the first workout, it is necessary to be completed by members the document of Health History. In this document, as can be easily assumed, there are personal data and sensitive personal data. The members are asked, about health problems, disabilities, weight and all the necessary information that a trainer have to know, in order to create an appropriate program that is tailored to needs and goals. The data that is collected is stored in a cloud server and the physical files are placed in cabinets that do not lock. Moreover, there are not a document destroyer and the documents are thrown in unsafe bins. According to Article 32 of GDPR, it is necessary the data to be stored in safe place where only the responsible staff members will have access. Moreover, based on articles 16 and 17 of the EU General

Data Protection Regulation the members have the right to erasure their data, something that is not easily can do.

4.3.3. Data of Potential Employees and Staff members

The Gym collects personal data of candidate employees. Candidates send their CV via email, which contains information about contact, education studies, professional experience, interests, photos etc. The CV are printed and stored as a physical file as well. Moreover, the data collects information from their employees in order to proceed the payroll process. The data which is collected has information about name, demographic data, taxis data, marital status and billing account.

4.3.4 Websites

As it has been reported the Gym has two websites. According to article 32, the websites have to encrypt data with SSL. Both of them are encrypted.

The first website it is used for the presentation of Gym facilities and services. The users may complete if they want, a contact form with some basic information (name, phone number, email). It is observed that there is not a privacy policy and the unsunbscription of the website is not easily available.

The second website collects and process personal data and sensitive personal data. During the period of Covid 19 and because of the lockdown the Gym resumed their operation for 3 months. Thus, it created a website in which the members participate in real-time trainings or to watch the practices in second time. In real-time training, members have the opportunity for audiovisual contact with the instructor as well as with the rest of website members who join the practice. The practices are recorded in order to be watched by the member in second time. Based on Articles 6,7 and 5, it is necessary the members to be well informed about the video recording, the purpose of it, the time-period that the video will be stored in the data base and to give their consent. The Gym, it refers clearly to the terms of use that every practice is recorded and moreover send an email with instruction in which it is clearly refer it.

In addition, the members have to complete the registration form in which state personal information (name, phone number, address, email) and a form that is related

to health history. The relevant data it is stored in a different data base of this that is been mentioned above. The website is aligned with the articles 16 and 17 of GDPR, and provide to their member the ability to erasure or process their data. Last but not least, based on article 6 of GDPR, the members give their consent to collect and process their data.

4.3.4 Web Analytics

The web analytics are a major sector in online marketing. According to articles 6 and 13 of GDPR it is necessary to be taken data subject consent and the web analytics purpose, process and store to be clearly referred into privacy policy. The websites' data of the Gym is linked to analytics tool. Thus, it has access valuable information and reports which is an important auxiliary factor for decision-making and a general overview of the users' behavior, desires and trends. The Gym collects visitor's data and creates relevant repots based on that data.

The Gym utilize the web analytics data, which is going to be examined below.

First and foremost, the Gym collects Audience data and Visitor Behavior's data. Via Web Analytics are collected valuable information about the total visits of the websites. With the help of IP addresses, it is extracted the Unique Visitors as well as the Returned Visitors. Last but not least, are collected information about the visitors who enters the website and then leave by doing any activity.

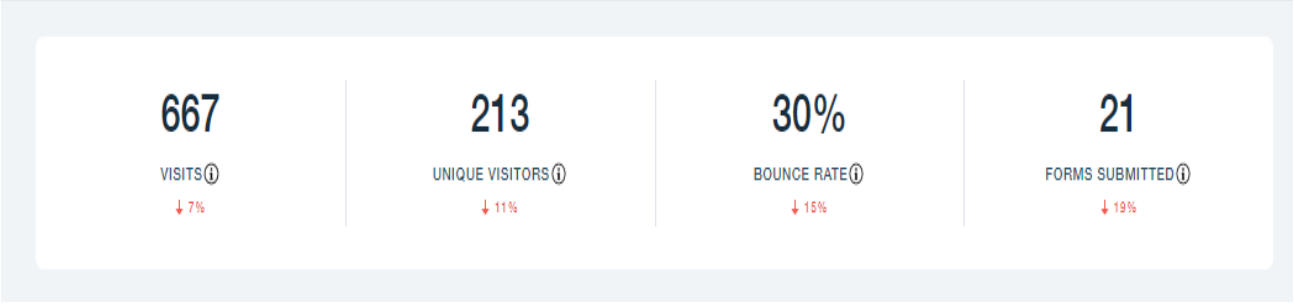

Figure 6_ Users Overview

Moreover, there is data about the total site visitors and the website traffic over time which can be extracted for any time period. In addition, web analytics collects data about the referring websites, an important information for marketing campaigns.

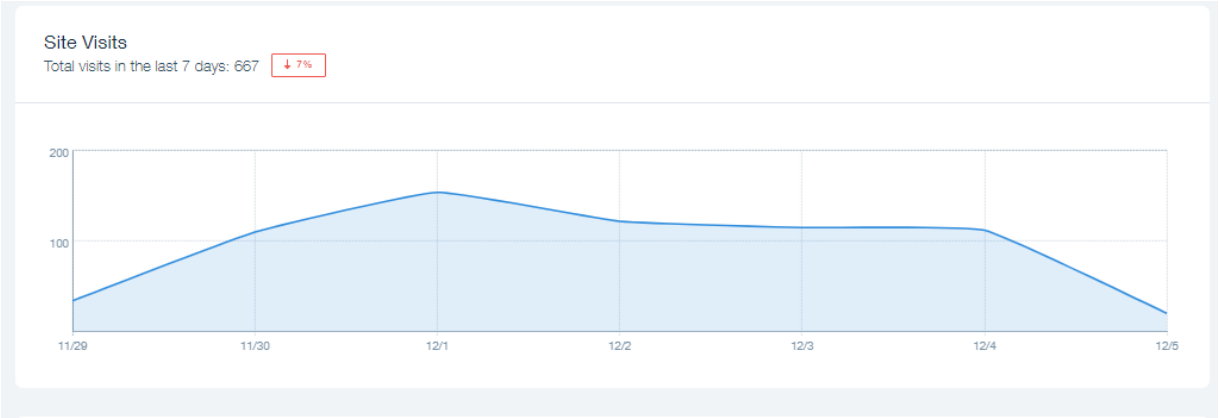

Figure 7_ Total Site Visits

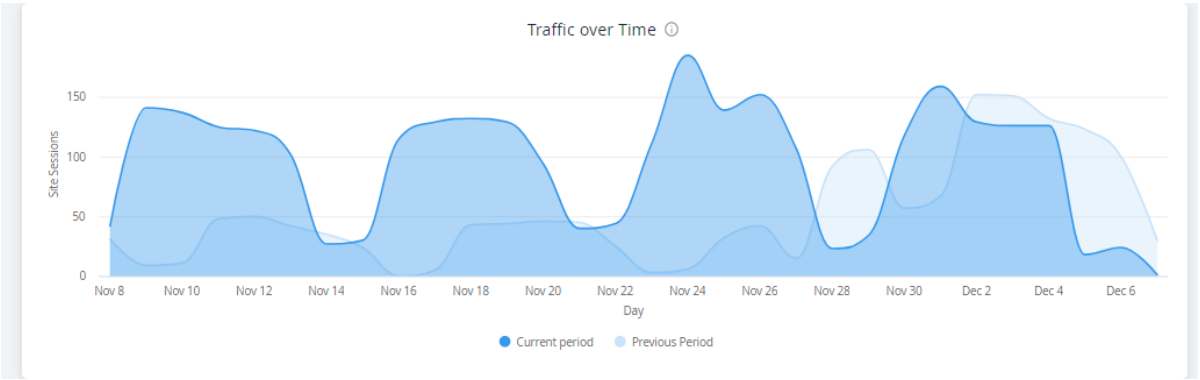

Figure 8_ Traffic over Time

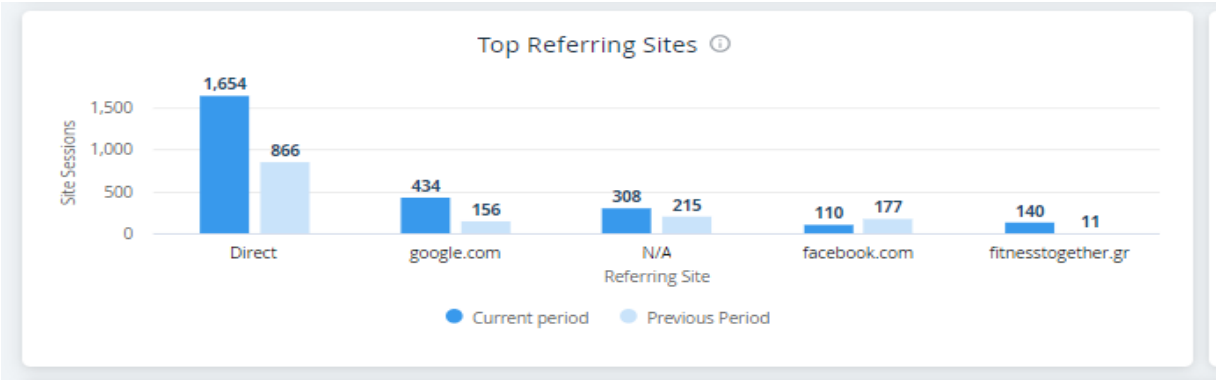

Figure 9_Top Referring Sites

Web Analytics provides valuable data about the returning and new users of the Gym's website.

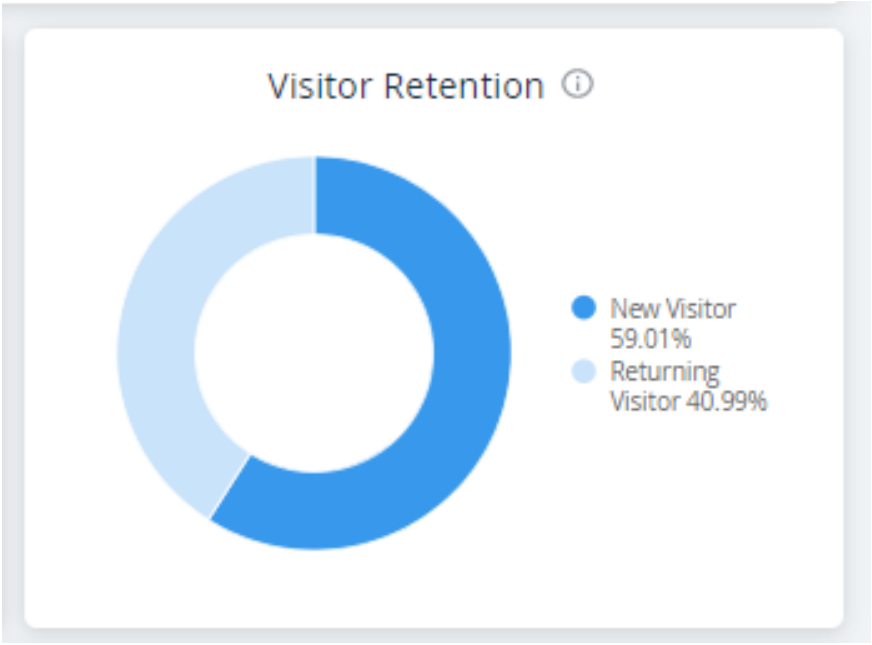

Figure 10_Visitors Retention

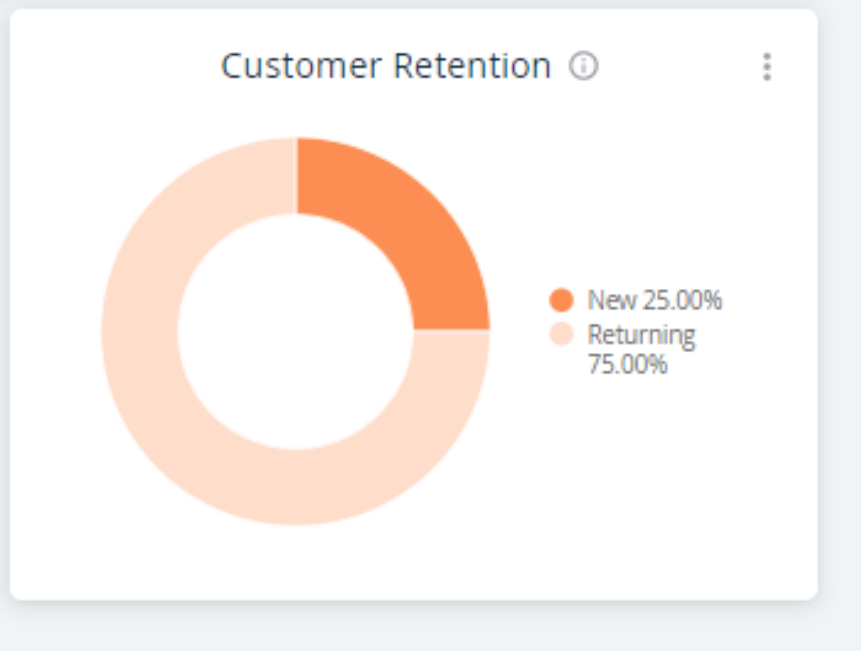

Figure 11_Customers Retention

Furthermore, it is collected demographic and Sales data. With the help of web analytics, Gym gain information about the top locations of traffic, the top client, the total sales and which courses are popular or not.

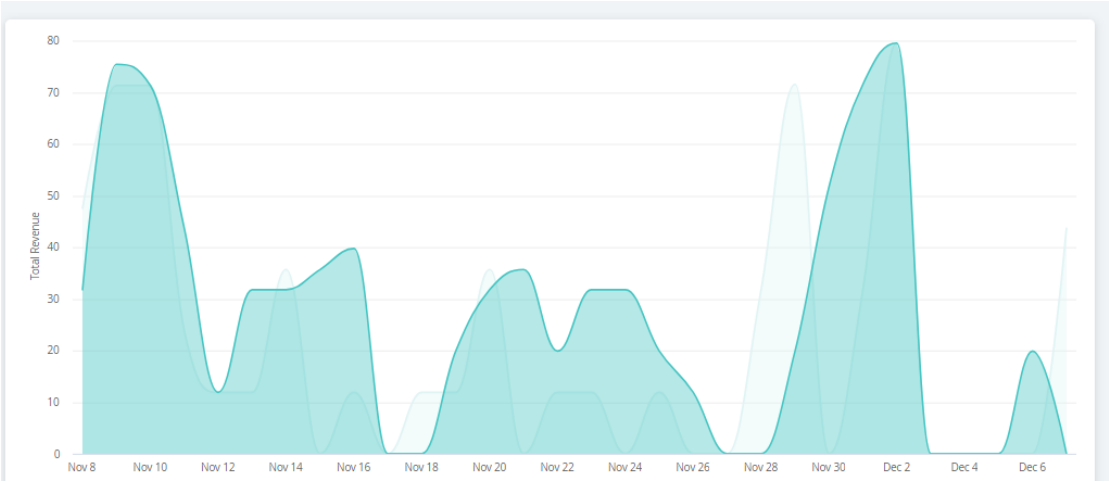

Figure 12_Sales over Time

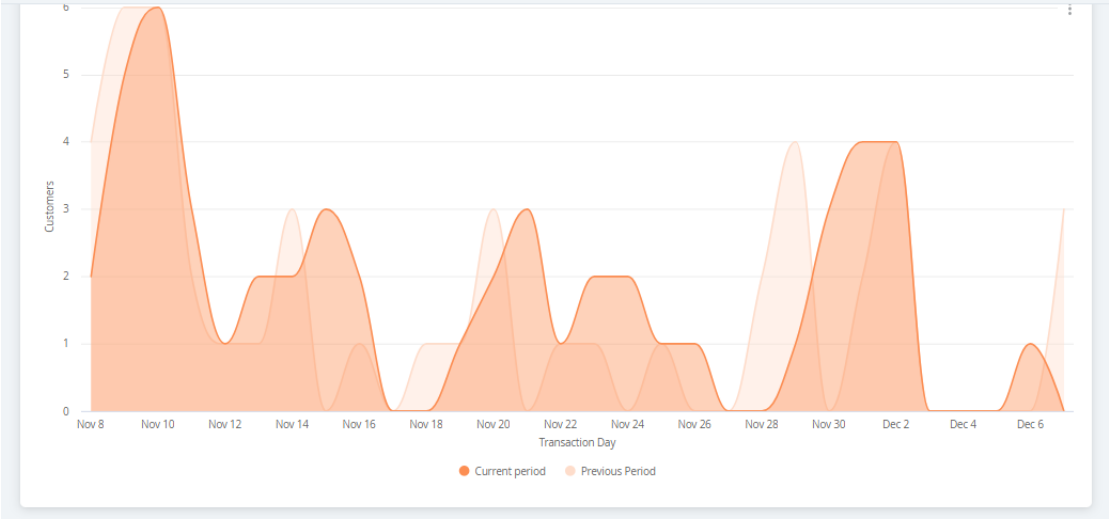

Figure 13_ Customers over Time

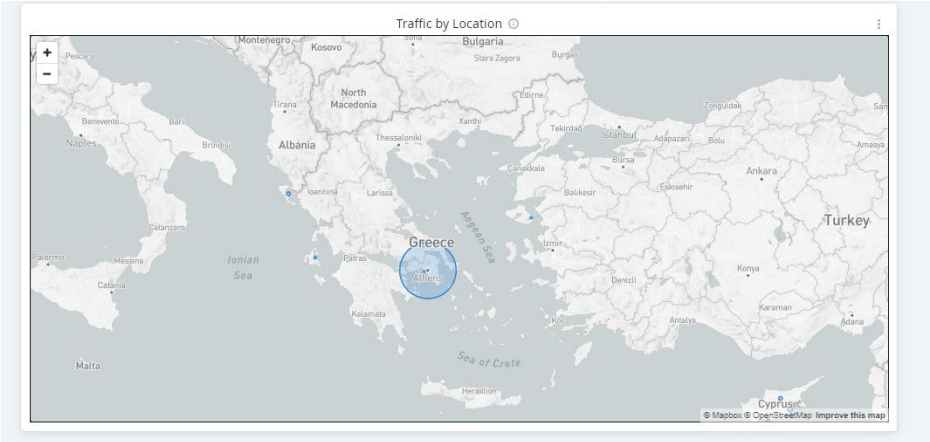

Figure 14_Traffic Location

All the Web Analytics data of the Gym contains personal data and must to comply with GDPR regulation.

4.4 Data processing and storage

According to Article 5 of the General Data Protection Regulation, in order the processing of personal data (personal data and "sensitive" personal data) to be legal, the processing must be governed by specific principles. These are:

1) **The principle of legality**, objectivity and transparency. According to this principle, data should be processed lawfully and fairly in a transparent manner in relation to the data subject. Transparency requires the information of the subject to be concise, easily accessible, understandable, with clear and simple wording.

2) **The principle of purpose limitation**, according to which data must be collected for specified, explicit and legitimate purposes and not be further processed in a manner incompatible with those purposes.
3) **The principle of proportionality "data minimization",** according to which data should be relevant and necessary for the intended processing purposes.
4) **The principle of data accuracy**, according to which data should be accurate and up-to-date.
5) **The principle of "integrity and confidentiality",** according to which data must be processed in a way that guarantees its security and protection from illegal processing, loss, destruction or deterioration.
6) **The principle of determining the duration of processing "limitation of the storage period",** according to which the data must be kept in a format that allows the identification of data subjects only for the time required to achieve the purposes of processing.
7) **The principle of data controller accountability**, according to which the controller bears the responsibility and should be able to demonstrate compliance with the Regulation before the supervisory authorities and the courts.

The Gym as it is mentioned above, process and store personal data and sensitive personal data.

4.4.1 Closed-circuit television (CCTV)

The data from the Closed-circuit television (CCTV) is processed by the Gym and the security company which is an external partner of the Gym. The security company is fully compliant with the regulations of the GDPR. The data are recorded for the safety of the Gym, staff and members. The recorded data is stored for one month in a cloud server in which have access the owner of the Gym and the data processor of the security company.

4.4.2 Registration of physical members

The data which is collected by the members during the Gym's registration are process via a CRM platform which is provided from an external IT company. The IT company is

complying with the Regulation. The CRM platform is on a cloud server and the access is completed remotely, by an encrypted and secure URL. Furthermore, there is a common password for all the Gym's employees and the access can be performed by all computers of the Gym. The data about the Health History of members are processed and stored into cloud and local server. The employees have access to computers via a common password. They access as administrators and not from a user's profile. All Gym's computers have antivirus system.

The physical files are stored in cabinets that do not have the ability to lock. In addition, they are not protected by the Closed-circuit television (CCTV) and are easily accessible even by the members of the Gym. In addition, there is no document shredder and documents containing personal data are thrown in the trash. Moreover, it is observed that there is no fire extinguisher in the document storage area.

The data of members is process for communication and marketing purposes. There is a relevant notification into the registration contract, in which the members can accept or deny.

Last but not least, the data are stored permanently and the members can process or delete their data by a relevant request to Gym's reception or via the booking application.

4.4.3 Booking Application and Check-In Process

4.4.3.1 Online Booking

The members of the Gym have the access to an online Booking Service which is connected to CRM platform, that has been analyzed above. The members are able to book a place into programs they desire, to get information about the total number of participants every program has and to chat with the Gym's receptionists for any request or question. The booking website is encrypted and safe. The members have access to the booking platform via unique username and password, which they obtain after their registration. The Gym collects and process the information about the member's booking, the training frequency or absence. These information are helpful about decision-making and marketing campaigns.

4.4.3.2 Check-In

During the member's entrance it is necessary to complete the check-in process. The check is completed by scanning their personal barcode, after that is presented into the screen a welcome message with their profile card. The profile card contains information about their name, contact information, the registration period and their last check-in. These information remain to the screen for fifteen seconds and are in common view with the rest members are in the reception area.

4.4.4 Websites

According to article 5, par. c of GDPR, the Gym collects the minimum data that is necessary in order to complete the purposes of collection. The main purpose of the process is to complete the members registration and to participate into the courses. Moreover, there are further data processes that take place after data collection. There is a relevant notification into the registration form that according to figure 15 it is pre-marked.

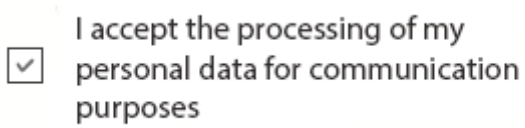

Figure 15_ Data Processing Consent

Considering article 7, par. 4 of GDPR the request for consent shall be freely submitted and in a way that is understandable and easily accessible format, using clear and simple wording.

The collected data from websites is processed by the Gym employees. First and foremost, the Gym, utilize the email and contact members information in order to promote marketing campaigns.

Moreover, the online purchases are processed by Stripe. Stripe is an online payment platform that allows businesses to send and receive payments over the Internet. Stripe is complying with GDPR rules.

Furthermore, as have been mention the online courses are recording for on-demand training purposes. The courses are stored in a cloud server and access to this server

has one of the Gym employees. During the online course the participants have open their cameras and have real-time communication with the instructor. The collected data is stored into cloud server for one month and then is stored in local server permanently. The members are informed about the recording via an email that receive after their online registration to courses as well as is written to the terms of use in the website.

4.4.5 Web Analytics

Based on article 5 of GDPR, the Gym has to explicitly state in simple words the data it collects and the purposes of their processing. Moreover, one of the key points of the Regulation is that the data subjects have to provide their consent about the data's collection and processing as well as should have easily the right to request the correction of personal data concerning them and the "right to be forgotten".

The Gym processes the data from web analytics tools in order to improve the usefulness of the websites and the services it offers, for marketing and remarketing purposes and for maximizing its profits.

The Gym collects data for two different analytics tools, Google Analytics and Wix Analytics. The owner of the Gym is the Data Controller and each tool is the Data Processor.

The first website it is connected with Google Analytics. Google Analytics uses a specific cookie format, which is stored on your computer and allows us to analyze the use of our website. Cookies provide significant help to the user friendliness of the website. It should be noted that Google Analytics has not been extended to this site to include "gat.anonymizeIp" code to ensure anonymous IP address logging (so-called IP masking). Google uses this information on behalf of the Gym to analyze the usage of the visitors of this website in order to prepare reports on the activities of the website and to provide additional services related to the use of the website and the internet. The reports mainly used in order to analyze and optimize the use of the website. The statistics obtained are used to improve the services offered and user's friendliness purposes.

It is observed that there is not a privacy policy in the website and the users are not able to request the correction of personal data concerning them and the "right to be forgotten". In addition, they are not been informed about their data processes and for how long the data is stored.

The second website it is connected with Wix Analytics tool. The data is processes and stored permanently in cloud server where the Data Controller has access. The exported reports and statistics are used for marketing and remarketing purposes in order to maximize profits of the online platform. Every New client is able to gain discount for the first month of registration. If a visitor signs up to the platform without accomplish registration, after two days receives an automate email with free seven days trial to online courses. Moreover, the collected data about the visitor's online behavior to the website it is used in order to be created as user-friendly environment as possible.

The collecting data sales provides a total overview about the platform's profits. Thus, the Gym is able to improve its strategic, to better understand the needs of its customer. The classification of data about the purchases per month, gender etc. helps the Gym to improve the decision making. In addition, the Gym utilize for marketing and remarketing purposes. Every six months, extracts information about the Top five customers and rewards them by providing them a free month of train to the platform. On the other hand, the users who do not reregister to the platform receives an automate thank-email with the request to complete a relevant evaluation.

4.4.6 Email Communication

The Gym is the administrator of two email accounts. Emails management programs are Gmail and Outlook. Access to these accounts have four members of the staff, who manage and process the emails. The emails are process personal and "sensitive" personal data Contact data, Demographic data, Subscription data, Medical data, Billing Data). The main purpose of the email accounts is for communication purposes with the customers, employees, suppliers and external partners. Moreover, emails accounts are used for advertisement purposes, for bulk sending emails to potential and existing members for information on Gym offers and services.

It is noticed that the employees are not educated according to GDPR, thus are observed that some bulk emails are sending to members without encryption (Bcc).

4.5 Gym Compliance with General Data Protection Regulation

This report includes the proposed organizational and technical safety measures as well as the proposed measures to improve the physical safety of the Gym. The proposed measures take into account the conclusions of the report on the recording of the current situation.

4.5.1 Proposed Organizational Security Measures

4.5.1.1 Organization / Personnel Management

The following is the proposed measure concerning the organization and management of Gym staff:

According to the article 37 of the General Regulation of Personal Data it is not necessary to be defined a Data Protection Officer, although based on article 39, b of GDPR about rolls assignment, it is recommended to be defined a Security Officer, a person.

Security Officer, is a person who has the responsibility to control and monitor policies and procedures related to the security of personal data and to take the necessary initiatives to eliminate all those factors that may jeopardize the availability, integrity and confidentiality of this data. It also oversees the implementation of all security measures and informs staff of any new safety instructions.

4.5.1.2 Staff Security Training.

A training and awareness program on security issues in the processing of personal data must be implemented in all the human resources of the Gym. A training employees' policy for the Protection of Personal Data should be developed and implemented. All employees of the Gym (existing and new) involved in the processing of personal data must be trained in the issues of personal data security, be aware of the Security Policy and the procedures and individual policies as well as the organizational and technical measures implemented by the Gym. Training should be continued after the

recruitment of new staff, either in the event of significant changes in security procedures or when significant security issues arise.

4.5.2 Proposed Technical Security Measures

4.5.2.1 Access control

According to article 6 of GDPR, the following are the proposed measures concerning the mechanisms and the control of access to the information systems maintained by the Gym:

- Enable password on all terminals. Activation of unique passwords per user, with complexity mechanisms, according to the password policy and assignment of access rights according to the role and responsibility of each user.
- The host server must be installed in a special area where only: The Gym owner and the Data Controller.

4.5.2.2 Backups

Based on the article 5 of GDPR, the Gym must design and implement a triple backup model. This model should include:

- The keeping of encrypted backups in the information systems (computers) of the Gym.
- Keeping encrypted backups on the host server used by the Gym.
- Keeping encrypted backups on a remote server (Cloud service), outside the Gym facility.

4.5.2.3 Computer Configuration

Below are presented the proposed measures related to the Gym's computers configuration in order to be aligned with the General Data Protection Regulation.

- Implementation of a central protection mechanism against malware of the terminals and central automatic download of updates of the respective protection software from a central server (anti-virus server) that serves the

Gym. Also, a central mechanism must be activated to record threats and monitor all computers on the network.

- Disable administrator rights from the terminals used by the employees of the Gym. Creation of user's profiles, thus every employee will access from a specific profile.
- Software upgrade.
- Upgrading the operating systems of the terminals with newer versions, which are fully compliant with the GDPR regulation.
- Upgrading and / or updating installed applications with newer ones that are compatible with privacy protection (e.g., Mozilla Firefox).
- Upgrade all Microsoft Office applications to the latest version.
- Hide screens displaying personal data

4.5.2.3 Websites

The following are the proposed measures regarding the websites maintained by the Gym:

- Installation of SSL certificate for protection and encryption of the website visitor data.
- Integration of privacy and security policy on the website.

4.5.2.3.1 Privacy Policy Example

Scope of the privacy policy

The Gym commits to preserve the privacy and confidentiality of all information provided by the user. The present Privacy Policy establishes the measures taken by The Gym concerning Personal Data collected directly from the user and/or through the site TheGym.com, in accordance with the Law on the Protection of Personal Data and other applicable legislation, both national and European.

The phrase "Personal Data" means all information concerning a natural person identified or identifiable, identifiable meaning a natural person that may be identified, directly or indirectly, especially by reference to an identifier, like for example a name, identification, location data, electronic identifiers or one or more specific elements of

the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Notice in case of changes to the privacy policy

The constant effort to improve the means and the adding of new functionalities to the site TheGym.com, as well as the existing services, meaning constant changes and improvements, changes to the legal applicable regime and evolution of technology, our practices, may entail changes as far as data treatment. When there is any change to the present Privacy Policy, The Gym will give notice to the User of their rights, and to the controlling authority responsible as required by law.

Acquis of personal data including e-mail address

To access certain services of the Gym website, the user may be required to provide the following data: name, address, e-mail address, telephone number, IBAN, tax payer number. They may also be requested to provide geographic information or aspects regarding personal preferences and interests of the user of the Gym website to allow The Gym to offer them a more customized service.

The information provided will be stored in the databases of The Gym, manually or by electronic means

Use of personal data

The Gym will provide the User with the information necessary to express prior consent to the treatment of their personal data for one or more specific purposes by The Gym and incorporation in the corresponding files owned by The Gym.

The data collected are processed automatically and aimed, within the corporate group that The Gym is part of, at establishing the quality of User/Client, consequent collection of vouchers and future contacts, namely direct marketing actions.

The data collected are also aimed at fulfilling legal obligations and use in contractual relations with Insurers, Banks and other Institutions, The Gym committing to keep the strict secrecy of all data, reserving access thereto as exclusively required for its normal activity.

The Gym may share, transfer or disclose the information of its database and server records in cases legally required, in the administration of justice, interacting with anti-fraud databases, to protect vital user interests, to protect the safety or integrity of our databases or site, to take measures against legal liability or, in case of sale, merger, reorganization, dissolution or otherwise of The Gym.

The Gym, as long as expressly authorized for that purpose by the holder of personal data, may transmit them to its trade partners, for advertising, marketing or promotional purposes. In case of breach by the User, the data may be transferred to third parties with the aim of debt collection.

The respective holder is ensured, in the terms of Law 67/98, of October 26th (Law on the Protection of Personal Data) the right to access and rectification thereof, as well as the right to object to the treatment of data for marketing purposes.

The information will be sent by The Gym to the address, e-mail or telephone contact provided by the user. The contacts provided will be preserved in our database and may be used to occasionally send information by e-mail or mail about products and services similar to those contracted by the user, deemed of interest thereto.

If the User does not wish to receive this type of information they must act in accordance with the chapter “Cancelation”. In cases in which the User has consented, their Personal Data may be shared with other companies of the same group as The Gym or said data may be disclosed to other companies that may contact the User about their products or services that may be of their interest.

The Gym, as long as duly authorized for the purpose by the holder of the data, may also treat it for the following purposes:

- Sending information about new products and services;
- Regular updates that The Gym deems of interest for the User;
- Sending requested information about products and services;
- For purposes of market studies and marketing;

- For internal use in the administration of the site TheGym.com and improvement of the services provided.

Rectification of data and corrections

To change their Personal Data, the User must send their request in writing and mention what data they wish to alter. We shall also correct and DELETE any Personal Data that is incorrect. Your data may be always updated through the contacts below.

Cancelation

If the user no longer wishes to receive e-mail from The Gym and wants out of the electronic mailing list, they may at any moment request that in any The Gym establishment or send an e-mail to the address, writing in the Subject "Cancelation of Mailing. If the User also wishes to be removed from the postal mailing list, they may do so tot the same e-mail address given above, writing in the subject "Postal Mailing Cancelation", or writing to our main office.

4.5.2.4 Email

Below are the suggested measures regarding the email communication, based on article 6 of GDPR

- Obtaining data subject consent
- Record keeping and obligation to prove the data subject consent
- Enable users to request the processing or deletion of their personal data.
- Sending emails to multiple recipients by using the Bcc (Blind Carbon Copy) function.
- Use of Digital Signature.
- Install DKIM (Domain Keys Identified Mail) signatures on emails. DKIM is an email security standard designed to make sure messages aren't altered in transit between the sending and recipient servers.
- Create separate business email accounts (Non-repudiation)

4.5.2.5 Web Analytics

According to article 37 of GDPR, the Gym is required to proceed to the following steps in order to be complied with the Regulation.

Cookie banner at the first visit of a user

The cookie notice must:

- Briefly explain the purpose of the installation of cookies are used.
- Clearly state which action will signify consent.
- Make available details of cookie purpose, usage, and related third-party activity.

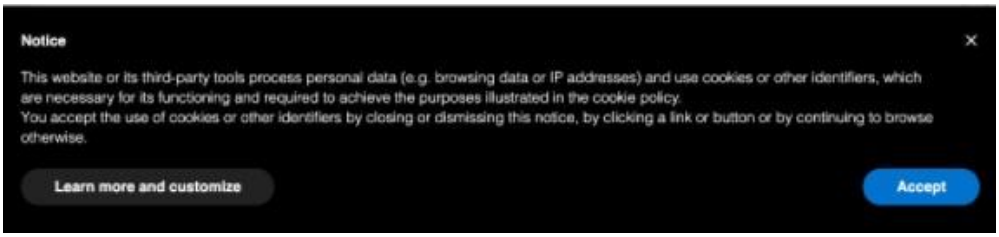

Figure 16_Cookies Notification

Implementing a cookie policy

- The cookie policy should:
- Clearly state the type of the cookies installed (e.g., statistical, advertising etc.).
- Description of the cookies purpose installation in details.

Consent to cookies

- Consent to cookies must be informed and explicit, and can be provided by a clear affirmative (opt-in) action. Therefore, mechanisms such as checkboxes, must not be pre-checked.

4.5.2.6 GDPR Security Policy

The Security Policy is a document of the data controller which describes the security objectives and the corresponding procedures to be followed in order to achieve these objectives. Defines the commitment of the Management and the approach of an organization or a company regarding the security of the information systems and networks and the protection of personal data kept by the data controller.

The security policy must, as a minimum, state the following:

- The basic principles that the data controller must follow, such as confidentiality, integrity and availability of data, accountability in case of errors and infringements, etc.
- The data (included files or equipment) that have to be protected.
- The purpose and scope of the security policy regarding the safeguarding of data and basic security principles.
- The organizational framework of roles, responsibilities, tasks related to security, as well as the staff's education about the GDPR compliance with it and the appropriate actions in case of violation.
- The internal control process, which should take place to review the proper implementation of the security policy and to assess the effectiveness of the security measures.

In case of the processing of personal data is completed by data processors, the security policy must specify its type, with simultaneous reference to the respective contract signed between the two parties. The processing time must also be stated in the security policy.

If part or all of the processing takes place exclusively on systems under the sole supervision of the processor, then this must be stated in the security policy. The part of the security policy concerning the processor must also be notified to him. In this case, the specific part of the security policy must explicitly state the obligation of the processor to fully adopt and implement it.

4.5.2.7 Security Plan

The Security Plan is the document that describes the organizational and technical measures, as well as the physical security measures that are applied and / or will be implemented to cover the basic principles and safety rules mentioned in the security policy, as well as the necessary actions for their implementation. It concerns both automated and non-automated data management and processing systems and must be applied precisely to protect personal data, sensitive or not, held by the controller.

In the Security Plan is accomplished regular reviews and revisions, given the rapid development of technological solutions and their application in information systems and technological infrastructure.

The Security Plan consists of the description of the personal data processing system, the organizational, technical security measures, as well as the physical security measures applied, the security implementation plan and the description of the procedures for continuous review and revision of the security plan.

4.5.2.8 Specific Technical Policies

4.5.2.8.1 Clean Desk Policy

Introduction

Clean Office Policy is one of the dominant strategies in the effort to reduce the risk of workplace safety violations and ensures that sensitive and confidential information does not exist in the workplace for no reason but is stored in a safe place when are not in use or when an employee leaves workplace. In addition, clean office policy increases the employee's perception of the protection of sensitive data.

Purpose

The purpose of this policy is to set the minimum requirements to maintain a "clean office" - where sensitive and critical information about customers or employees are kept secure, locked out of the workplace.

Application Field

This policy applies to the employees of the Company under the name "The Gym" based in Thessaloniki

Policy

- Employees are required to ensure that all sensitive and confidential data, in printed or electronic form is secure at their workplace at the end of the day and when they are expected to be missing for an extended period of time.
- Computer workstations must be locked when the workspace is unoccupied.
- Any kind of restricted or sensitive information should be removed from the desk and locked in a drawer when no one is at the desk at the end of the workday.
- Keys used to access restricted or confidential information should not be left unattended in an office.
- Laptops or tablets must be either locked with a security cable or locked in a drawer.
- In case of destruction of documents with limited or sensitive content, they should be shredded in the official shredding bins or placed in locked, confidential waste bins.
- Mass storage devices such as CDROMs, DVDs, or USB drives that contain sensitive data must be secured in a locked drawer.

- All printers and fax machines should be cleaned of paper as soon as they are printed. This helps to make sure that no sensitive documents remain on the printer trays for the wrong person to pick them up.

Compliance with Policy

Conformity measurement

The Information Security Officer is responsible for ensuring that employees comply with this policy through a program of audits carried out at certain intervals.

Non-compliance

An employee of the Company who is found to have violated this policy may be subject to disciplinary action, including termination of employment with the Company

4.5.2.8.2 Employees Internet Usage Policy

Purpose and Brief Description of the Policy

The internet usage policy of the employees describes the instructions for the use of the internet in order to avoid the inappropriate or illegal use of the internet, which creates risks for the legality and the reputation of the Gym. This internet policy applies to all employees and external partners who have access to the network and computers.

Policy Implementation

What is the proper use of the internet by employees?

The Company recommends that employees use the internet connection for the following reasons:

- To complete their tasks.
- Search for information they can use to improve their work.
- Connect to the platforms and account of the Gym.

Any use of the network and connection must follow our privacy and data protection policy.

Employees must:

- Keep passwords secret in any case.
- Log in to corporate accounts only from secure devices.
- Use strong passwords to log in to work-related websites and services.

Employees must not use the Company's network to:

- Send confidential information to unauthorized recipients.
- Violate the privacy and sensitive information of another person.
- "Download" movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that may endanger the security of the Company's network
- Perform unauthorized or illegal activities, such as hacking, fraud, buying / selling illegal goods

Illegal Activity

Employees who do not comply with this Internet Use Policy will face disciplinary action.

Serious violations can result in dismissal of the employee.

Examples of serious violations are:

- Using the internet connection to steal or engage in other illegal activities.
- Infecting your computer with viruses or other malware.

4.6 Personal Data Breach Procedure

Pursuant to article 33 of the Regulation, in the event of personal data breach, the data controller shall promptly and, if possible, within 72 hours of becoming aware of the personal data breach to the supervisory responsible authority in accordance with Article 55, unless the breach of personal data does not endanger the rights and freedoms of individuals. Accordingly, if the infringement of personal data may endanger the rights and freedoms of individuals, the data controller shall promptly notify the breach event of the personal data to the data subject.

4.6.1 Risk identification

What are considered incidents of security breach:

- The disclosure of personal data to unauthorized persons
- The loss or theft of mobile devices or equipment containing personal, confidential or sensitive data
- Loss or theft of a physical file
- Violation of the company's security policy

- Unauthorized access and modification or deletion of files.
- Spread of viruses or other security attacks on computer systems or networks.
- Physical security breaches.
- Unsafe disposal of waste paper with personal data.
- Publishing confidential data on the internet by mistake and accidentally disclosing passwords.
- Sending erroneous emails or faxes containing personal, confidential or sensitive data.

4.6.2 Reporting Incidents Process of Personal Data Breach

If a personal data breach occurs and is detected by a staff member, the personal data breach report must be completed.

Once the report has been received by the security officer, the significance of the incident is assessed.

4.6.3 Breach Notification to the Authority

For the notification of a violation case to the Authority, in compliance with the relevant obligation of no. 33 of Regulation (EU) 2016/679, the controller must fill in a special form and submit it to the Authority electronically *, by sending to the e-mail address: databreach@dpa.gr

4.6.4 Breach Notification to the Data Subjects

When the breach of personal data may seriously endanger the rights and freedoms of individuals, according to the above assessment, the data controller shall promptly notify the breach of personal data to the data subject.

The communication to the data subjects includes the following:

- Description of the nature of the breach of personal data.
- Announcement of the name and contact details of the person with whom they can contact for more information.
- Description of the possible consequences of the personal data breach.

- Description of the measures taken or proposed to be taken by the company to deal with the breach of personal data, and, where appropriate, measures to mitigate any adverse effects.

4.6.5 Breach Report on the Record of Violation

It is necessary the breach event to be reported to the Violation Record which is retained by the Gym. The information which are necessary to be completed are the following:

- Date of Violation
- Time of violation
- Description of Violation
- Date of notification of the violation to the Supervisory Authority
- Time elapsed until the notification
- Possible Consequences for Data Subjects
- Corrective actions

4.6.6 Personal Data Breach Management Chart

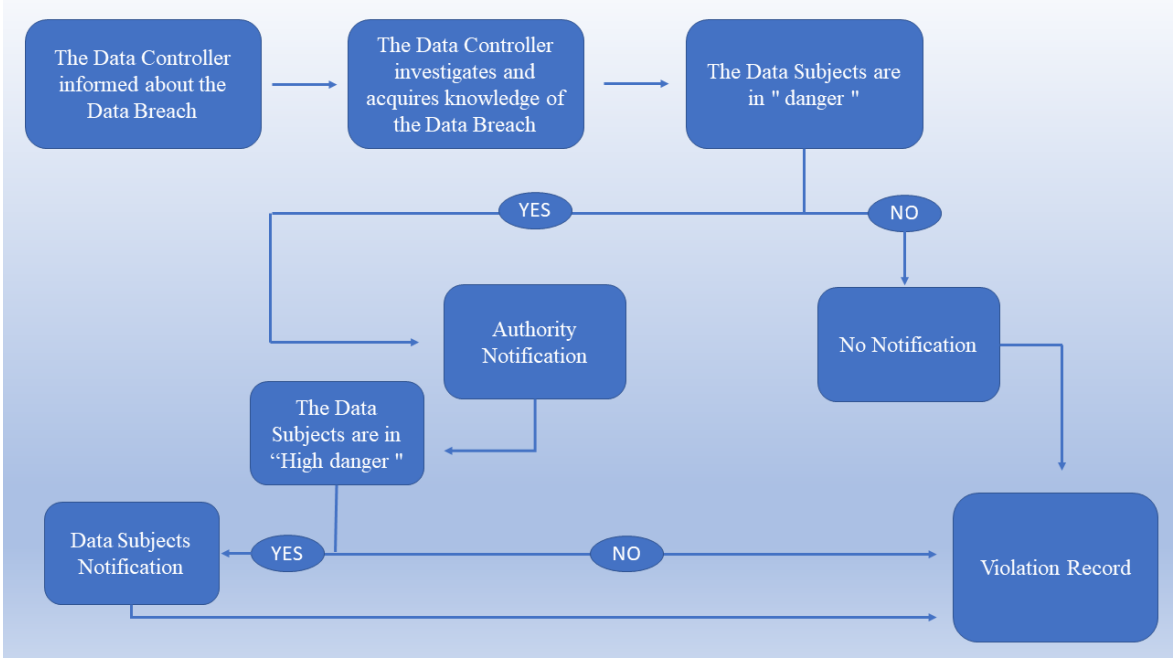

Figure 17_ Personal data breach management chart

Conclusions

In recent years it is indisputable that the regulation is a controversial issue which has preoccupied and brought significant changes in the operation of companies which process data of EU citizens. Although regulations for the processing of personal data have existed for about 30 years, the important thing about the GDPR is that it brings large fines to companies that do not comply. The Regulation introduces new obligations in both the physical operation of a business and the digital one. From a small company, like the Gym that have been analyzed above, to a large enterprise like Amazon the GDPR protects the personal data and the rights of citizens. The time and effort required to achieve compliance will vary greatly from one organization to another, but it is well worth the effort.

Bibliography

1. B.Gerhardt, K. Griffin and R. Klemann, "Unlocking Value in the Fragmented World of Big Data Analytics", Cisco Internet Business Solutions Group, June 2012
2. C. Eaton, D. Deroos, T. Deutsch, G. Lapis and P.C. Zikopoulos, Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data, Mc Graw-Hill Companies, 978-0-07-179053-6, 2012
3. S. Singh and N. Singh, "Big Data Analytics", 2012 International Conference on Communication, Information & Computing Technology Mumbai India, IEEE, October 2011
4. Edd Dumbill (O'Reilly Media), "Volume, Velocity, Variety: What You Need to Know About Big Data"
5. W. Christl and S. Spiekermann, Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Facultas, 2016. [Online]. Available: https://books.google.it/books?id=sE45vgAACAAJ
6. G. D. Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y. de Montjoye, and A. Bourka, "Privacy by design in big data – an overview of privacy enhancing

technologies in the era of big data analytics," ENISA Report, V 1.0, 2015, https://www.enisa.europa.eu/publications/big-data-protection.

7. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
8. D. Riboni, L. Pareschi, C. Bettini, JS-Reduce: defending your data from sequential background knowledge attacks, IEEE Trans. Dep. Sec. Comp., 9 (2012) 387-400.
9. Boris Lubarsky, "re-identification of "anonymized data", cite as: 1 geo. l. tech. rev. 202 (2017)
10. Id. at 1720; The Netflix Prize Rules, NETFLIX, http://www.netflixprize.com/rules (last visited June 12, 2010) [https://perma.cc/RA6L-LB8B]
11. John Bohannon "Genealogy Databases Enable Naming of Anonymous DNA Donors" January 2013
12. C. Duhigg," How companies learn your secrets", New York Times Magazine,2012
13. Bi, Z. M., Xu, L. D., & Wang, C. (2014). Internet of Things for enterprise systems of modern manufacturing. IEEE Transactions on Industrial Informatics.
14. Bloem, J., Doorn, M. van, Duivestein, S., Manen T. van, Ommeren, E. van, & Sackdeva, S. (2013). No more secrets with big data analytics.
15. M. Vijayalakshmi,V.E.S.I.T, Chembur ,(2014), Big Data Analytics Frameworks.
16. Haina Ye, Xinzhou Cheng, Mingqiang Yuan, Lexi Xu, Jie Gao, and Chen Cheng,"A Survey of Security and Privacy in Big Data",2016
17. Big Data Public Private Forum, "Big Data Technical Working Groups White Paper," 2014.
18. (W. S Zheng, Gong, S., and T. Xiang, "Person re-identification by probabilistic relative distance comparison," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Providence, 2011
19. O. Tene and J. Polonetsky, "Judged by the Tin Man: Individual Rights in the Age of Big Data," Journal of Telecommunications and High Technology Law, 2013.

20. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). doi:10.1007/978-3-319-57959-7
21. Team, I. G. P. (2020). Eu general data protection regulation (gdpr)–an implementation and compliance guide. IT Governance Ltd.
22. Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. Information Systems, 91, 101469.
23. Cheimonidis, P. (2019). The responsibilities of the DPO according to the GDPR.
24. Smouter-Umans, K. L. (2017). Research, GDPR, and the DPO How GDPR Changes the Game for Those Conducting Research and the Data Supervisors. Int'l J. Data Protection Officer, Privacy Officer & Privacy Couns., 1, 26.
25. Canard, S., Guilloteau, S., & Boudet, F. (2013). U.S. Patent No. 8,607,332. Washington, DC: U.S. Patent and Trademark Office.
26. Song, D. X., Wagner, D., & Perrig, A. (2000, May). Practical techniques for searches on encrypted data. In Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000 (pp. 44-55). IEEE.
27. Lieberman, J. D., Koetzle, D., & Sakiyama, M. (2013). Police departments' use of Facebook: Patterns and policy issues. Police quarterly, 16(4), 438-462.
28. Million Euro Fine for Data Protection Violations in H&M's Service Center (2020) Available: https://datenschutz-hamburg.de/assets/pdf/2020-10-01-press-release-h+m-fine.pdf?lspt_context=gdpr
29. LinkedIn Lost 167 Million Account Credentials in Data Breach,2016, Available: https://fortune.com/2016/05/18/linkedin-data-breach-email-password/#:~:text=LinkedIn.
30. Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. The European Physical Journal B, 89(1), 1-12.
31. Regulation, G. D. P. (2018). General data protection regulation (GDPR). Intersoft Consulting, Accessed in October 24, 1.
32. Team, I. G. P. (2020). Eu general data protection regulation (gdpr)–an implementation and compliance guide. IT Governance Ltd.

33. Jensen, M. (2013, June). Challenges of privacy protection in big data analytics. In 2013 IEEE International Congress on Big Data (pp. 235-238). IEEE.
34. Goldberg, S., Johnson, G., & Shriver, S. (2019). Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes. Available at SSRN 3421731.
35. Sørensen, J., & Kosta, S. (2019, May). Before and after gdpr: The changes in third party presence at public and private european websites. In The World Wide Web Conference (pp. 1590-1600).
36. Zoltán, P. B., Isabella, S. Z. Ő. C. S., & Anna, M. J. GDPR and Website Compliance. Mihnea S. STOICA Andreea VOINA, 125.
37. Park, J. S., & Sandhu, R. (2000). Secure cookies on the Web. IEEE internet computing, 4(4), 36-44.
38. Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016, April). An empirical study of web cookies. In Proceedings of the 25th International Conference on World Wide Web (pp. 891-901).
39. Spain: Cookie-Banner causes 30.000€ fine for Vueling Airlines,Availiable: https://easygdpr.eu/gdpr-incident/spain-cookie-banner-causes-30-000e-fine/
40. Smith, M., Szongott, C., Henne, B., & Von Voigt, G. (2012, June). Big data privacy issues in public social media. In 2012 6th IEEE international conference on digital ecosystems and technologies (DEST) (pp. 1-6). IEEE.
41. Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018, December). Privacy issues and data protection in big data: a case study analysis under GDPR. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 5027-5033). IEEE.
42. https://www.facebook.com/policies/cookies/
43. Gomer, R., Rodrigues, E. M., Milic-Frayling, N., & Schraefel, M. C. (2013, November). Network analysis of third party tracking: User exposure to tracking cookies through search. In 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT) (Vol. 1, pp. 549-556). IEEE.

44. Chaffey, D., & Patron, M. (2012). From web analytics to digital marketing optimization: Increasing the commercial value of digital analytics. Journal of Direct, Data and Digital Marketing Practice, 14(1), 30-45.
45. Zheng, G., & Peltsverger, S. (2015). Web analytics overview. In Encyclopedia of Information Science and Technology, Third Edition (pp. 7674-7683). IGI Global.
46. Phippen, A., Sheppard, L., & Furnell, S. (2004). A practical evaluation of Web analytics. Internet Research.

Appendix

Record of Processing Activities of "the Gym"

Record of Processing Activities of "the Gym"		
Processing Activity Name	**Closed-circuit television (CCTV)**	
Data Subjects' categories	Clients, Employees	Clients, Potential clients
Data Types categories	Personal Data (Physiological Data)	Personal data and Sensitive Personal Data(Contact data, Demographic data, Subscription data, Medical data.)
Lawful basis	Art 6,par 1,f of GDPR	Art 6,par 1,b of GDPR
Purpose	Security of facilities, employees and customers	Gym Registration
Data retention period	1 month	Permanently
Physical place or information system of personal data protection	Logical access control	Logical and physical access control
General description of organizational and technical security measures	Digital video recorders (DVRs) are stored in local server, in a private room. Access to this rooms has only the Gym owner. In the rooms there is fire extinguisher	Physical Files are stored in unlocked cabinets, in Gym reception. There are cameras and fire extinguisher the rooms but there is not document destroyer. The logical files are stored in cloud in CRM system which is comply with GDPR. There is a common password for every user.

Data Processor	The Gym	the Gym
Data Receiver	The Gym	the Gym
Owner Name	The Gym	the Gym
Processing Activity Name	**Online Registration Process**	**Recording of Real-Time Training courses**
Data Subjects' categories	Clients	Instructors and Clients
Data Types categories	Personal data and Sensitive Personal Data(Contact data, Demographic data, Subscription data, Billing Data, Medical data.)	Personal Data (Physiological Data)
Lawful basis	Art 6,par 1,b of GDPR	Art 6,par 1,f of GDPR
Purpose	Registration to real time training courses	On-Demand training
Data retention period	Permanently	Permanently
Physical place or information system of personal data protection	Logical access control	Logical access control
General description of organizational and technical security measures	The data is stored in a cloud server which is comply with GDPR.Access to database have the Gym owner and the data controller. The website is comply with GDPR.	The data is stored in a cloud server which is comply with GDPR.Access to database have the Gym owner and the data controller. The website is comply with GDPR.
Data Processor	The Gym	The Gym
Data Receiver	The Gym	The Gym
Owner Name	The Gym	The Gym
Processing Activity Name	**Advertising Campaigns**	**Communication via Email**
Data Subjects' categories	Clients, Potential Clients	Clients, External Partners, Suppliers, Employees
Data Types categories	Personal data(contact data,demografic data)	Personal data and Sensitive Personal Data(Contact data, Demographic data, Subscription data, Medical data, Billing Data)
Lawful basis	Art 6,par 1,f of GDPR	Art 6,par 1,e of GDPR
Purpose	Advertising of offers and services of the Gym. Maximize Profits	Communication with clients,suppliers,employees and external partners
Data retention period	Permanently	Permanently

Physical place or information system of personal data protection	Logical access control	Logical access control, Microsoft Outlook,Gmail
General description of organizational and technical security measures	Encrypted email marketing. Notification of unsubscribing. The data were collected with the subjects' consent.	Password,SSL encryption
Data Processor	The Gym	The Gym
Data Receiver	The Gym	Clients, External Partners, Suppliers, Employees
Owner Name	The Gym	The Gym
Processing Activity Name	**Website Administration**	**Collection and retention of CVs**
Data Subjects' categories	Website Visitors	Potential Employees
Data Types categories	Personal Data (IP adress, Email, Web Analytic's Data)	Personal Data(Name, patronymic, patronymic, address, gender, age, identity, place of birth, married / unmarried, number of children, education, qualifications, telephone number, photo, previous service)
Lawful basis	Art 6,par 1,a of GDPR	Art 6,par 1,f of GDPR
Purpose	website promotion and membership increase	Collection and storage of CV data for evaluation and possible recruitment
Data retention period	permanently	permanently
Physical place or information system of personal data protection	Logical and physical access control	Logical access control
General description of organizational and technical security measures	Website compliance with GDPR, cookies policy, SSL encryption, Unsunscription right	firewall, antivirus, back up to external hard drive
Data Processor	The Gym	The Gym
Data Receiver	The Gym	The Gym
Owner Name	The Gym	The Gym
Processing Activity Name	**Payrolls**	
Data Subjects' categories	Employees	

Data Types categories	Personal data(name, demographic data, taxis data, marital status,billing account)	
Lawful basis	Art 6,par 1,b of GDPR	
Purpose	Employees payment	
Data retention period	permanently	
Physical place or information system of personal data protection	The data is stored in physical and logical files. It is stored in cabinets and in local server. Password.	
General description of organizational and technical security measures	The data is processes of an account company which is an external partner of the Gym in order to be completed the payroll procees	
Data Processor	The Gym	
Data Receiver	Accounting company	
Owner Name	The Gym	